(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2001－195509
（P2001－195509A）
(43)公開日　平成13年７月19日(2001.7.19)

(51)Int.Cl.'	識別記号	ＦＩ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ	
Ｇ１０Ｋ　15/02		Ｇ１０Ｋ　15/02		

審査請求　未請求　請求項の数６　ＯＬ　（全 32 頁）

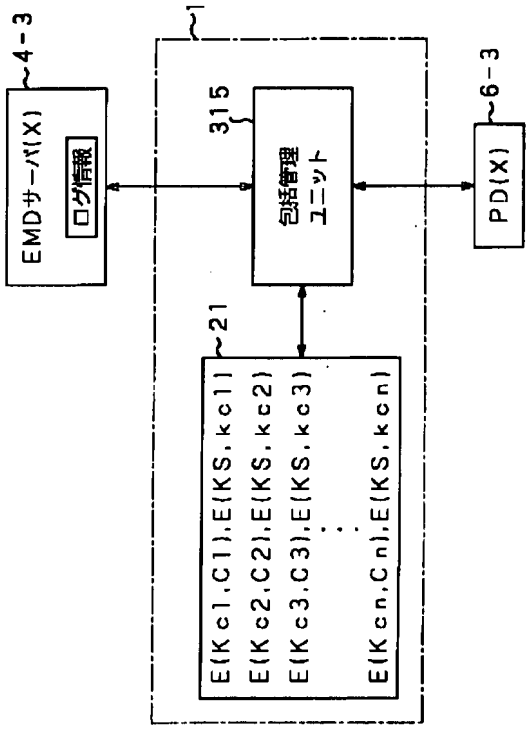
(21)出願番号　特願2000－326125(P2000－326125)
(22)出願日　平成12年10月25日(2000.10.25)
(31)優先権主張番号　特願平11－303138
(32)優先日　平成11年10月25日(1999.10.25)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　石黒　隆二
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　河上　達
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100067736
弁理士　小池　晃　（外２名）

最終頁に続く

(54)【発明の名称】　コンテンツ提供システム、コンテンツ配信方法、及び、記憶媒体

(57)【要約】
【課題】　ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元する。
【解決手段】　ＰＣは、配信された音楽コンテンツのバックアップをハードディスクに記憶するとともに、ハードディスクに格納している音楽コンテンツの使用ログ情報をＥＭＤサーバに送信する。ＰＣは、例えばハードディスク内の音楽コンテンツが破壊したときには、使用ログ情報をＥＭＤサーバから取得し、使用ログ情報に応じてハードディスクに記憶しているバックアップデータの再生をする。



【特許請求の範囲】

【請求項１】　コンテンツデータをネットワークを介して配信するコンテンツサーバと、
コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、
上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とするコンテンツ提供システム。

【請求項２】　コンテンツデータをネットワークを介して配信するコンテンツサーバと、
コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、
上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とするコンテンツ提供システム。

【請求項３】　コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、
上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、
上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに、配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、
上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、上記使用ログ情報を上記データ処理装置に送信し、
上記データ処理装置が、上記使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とするコンテンツ配信方法。

【請求項４】　コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、
上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、
上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、
上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、この取得できなくなったコンテンツデータを上記データ処理装置に再配信するとともに、上記使用ログ情報を上記データ処理装置に送信し、
上記データ処理装置が、上記使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とするコンテンツ配信方法。

【請求項５】　データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、
上記再生制御プログラムは、
上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とする記憶媒体。

【請求項６】　データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、
上記再生制御プログラムは、
上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータ

を上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークを介して音楽データ等のコンテンツデータを提供するコンテンツ提供システム、コンテンツ配信方法、及び、記憶媒体に関するものである。

【０００２】

【従来の技術】近年、インターネットやケーブルテレビ等のネットワークを用いた音楽コンテンツのオンライン配信が実用化され始めた。

【０００３】このような音楽コンテンツの配信システムにおいては、コンテンツ配信業者は、音楽コンテンツをネットワークを介して配信する場合、例えば、Ｗｅｂ上に音楽コンテンツを提供する。また、この音楽配信システムを利用するユーザは、自己のパーソナルコンピュータを用いて、コンテンツ配信業者が提供するＷｅｂ等にアクセスをして、所望の音楽コンテンツをダウンロードする。

【０００４】

【発明が解決しようとする課題】ところで、このような音楽配信システムにおいては、一般に、ダウンロードした音楽コンテンツに対して例えばネットワークを介して課金がされる。

【０００５】しかしながら、例えば、ユーザが保有するパーソナルコンピュータ内のデータが破壊してしまうと、一旦購入した音楽コンテンツも消滅してしまう。そのため、その音楽コンテンツを復元させるには、再度、コンテンツを購入しなければならなかった。

【０００６】本発明は、このような実情を鑑みてなされたものであり、ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元することができるコンテンツ提供システム、コンテンツ配信方法、及び、記憶媒体を提供することを目的とする。

【０００７】

【課題を解決するための手段】本発明にかかるコンテンツ提供システムは、コンテンツデータをネットワークを介して配信するコンテンツサーバと、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とする。

【０００８】コンテンツ提供システムでは、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元データの再生及び／又は制御を行う。

【０００９】本発明にかかるコンテンツ提供システムでは、コンテンツデータをネットワークを介して配信するコンテンツサーバと、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とする。

【００１０】このコンテンツ提供システムでは、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、再配信されたコンテンツデータの再生及び／又は制御を行う。

【００１１】本発明にかかるコンテンツ配信方法は、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに、配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、上記使用ログ情報を上記データ処理装置に送信し、上記データ処理装置が、上記使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とする。

【００１２】このコンテンツ配信方法では、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元データの再生及び／又は

制御を行う。

【００１３】本発明にかかるコンテンツ配信方法は、コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、この取得できなくなったコンテンツデータを上記データ処理装置に再配信するとともに、上記使用ログ情報を上記データ処理装置に送信し、上記データ処理装置が、上記使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とする。

【００１４】このコンテンツ配信方法では、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、再配信されたコンテンツデータの再生及び／又は制御を行う。

【００１５】本発明にかかる記憶媒体は、データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、上記再生制御プログラムは、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすることを特徴とする。

【００１６】この記憶媒体では、再生制御プログラムがインストールされたデータ処理装置に対して、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元データの再生及び／又は制御を行わせる。

【００１７】本発明にかかる記憶媒体は、データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、上記再生制御プログラムは、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすることを特徴とする。

【００１８】この記憶媒体では、再生制御プログラムがインストールされたデータ処理装置に対して、コンテンツサーバから再取得した使用ログ情報に基づき、再配信されたコンテンツデータの再生及び／又は制御を行わせる。

【００１９】

【発明の実施の形態】以下、本発明の最良の実施の形態として、本発明を適用した音楽コンテンツ配信システムについて図面を参照しながら詳細に説明する。この音楽コンテンツ配信システムは、ネットワークを介してサーバからパーソナルコンピュータやポータブルデバイスにダウンロードし、さらに、ダウンロードした音楽コンテンツやＣＤから読みとった音楽コンテンツの管理等を行うシステムである。

【００２０】（１）音楽コンテンツ配信システムの全体構成

図１は、本発明を適用した音楽コンテンツ配信システムの全体構成を示す図である。

【００２１】この音楽コンテンツ配信システムは、パーソナルコンピュータ１と、インターネットやローカルエリアネットワーク等のネットワーク２と、登録サーバ３と、音楽データ（以下、コンテンツと呼ぶ。）を配信する複数のＥＭＤ（ Electrical Music Distribution ）サーバ４（４－１，４－２，４－３）と、WWWサーバ５（５－１，５－２）とを備えて構成される。また、パーソナルコンピュータ１には、ＵＳＢケーブル７（７－１，７－２，７－３）を介して、内部にメモリーカード等の記憶媒体が格納され、コンテンツの再生を行う携帯型の音楽再生器機であるポータブルデバイス６（６－１，６－２，６－３）が接続される。

【００２２】パーソナルコンピュータ１は、ネットワーク２を介して、ＥＭＤ登録サーバ３、ＥＭＤサーバ４（４－１，４－２，４－３）、WWW（ World Wide Web ）サーバ５（５－１，５－２）と接続される。

【００２３】パーソナルコンピュータ１は、ＥＭＤサーバ４（４－１，４－２，４－３）から、所定の圧縮方式で圧縮されたコンテンツを受信し、所定の暗号化方式で暗号化して記録する。また、パーソナルコンピュータ１は、ＣＤ（ Compact Disc ）等から読みとったコンテンツを、所定の圧縮方式で圧縮して、所定の暗号化方式で暗号化して記録する。圧縮方式としては、例えばＡＴＲＡＣ（ Adaptive Transform Acoustic Coding ）３（商標）やＭＰ３（ MPEG Audio Layer -3）等の方式が用い

られる。また、暗号化方式としては、ＤＥＳ（Data Encryption Standard）などが用いられる。

【００２４】また、パーソナルコンピュータ１は、コンテンツの配信を受ける場合には、そのコンテンツの利用条件を示す利用条件情報の配信も受け、それを記録する。また、パーソナルコンピュータ１は、ＣＤ等から読みとったコンテンツを記録する場合には、そのコンテンツの再生条件に応じて、利用条件情報を生成して、それを記録する。

【００２５】また、パーソナルコンピュータ１は、暗号化して記録しているコンテンツを、利用条件情報及び曲名や演奏者等の関連情報とともに、ＵＳＢケーブル７（７－１，７－２，７－３）を介して、ポータブルデバイス６（６－１，６－２，６－３）に記録し、記憶させたことに対応して利用条件情報を更新する。この処理のことをチェックアウトという。利用条件情報は、チェックアウトしたとき、パーソナルコンピュータ１が記録している、そのコンテンツのチェックアウト可能回数を１減少させる。チェックアウト可能回数が０のときには、対応するコンテンツは、チェックアウトすることができない。

【００２６】また、パーソナルコンピュータ１は、ＵＳＢケーブル７（７－１，７－２，７－３）を介して、ポータブルデバイス６（６－１，６－２，６－３）に記憶されているコンテンツを、消去し（または、使用できなくさせ）、消去したことに対応させて利用条件情報を更新する。この消去処理のことをチェックインと呼ぶ。チェックインしたとき、パーソナルコンピュータ１が記録している、そのコンテンツのチェックアウト可能回数を１増加させる。

【００２７】なお、パーソナルコンピュータ１は、他のパーソナルコンピュータがポータブルデバイス６にチェックアウトしたコンテンツに対してはチェックインはできない。すなわち、パーソナルコンピュータ１自身がチェックアウトしたコンテンツしか、チェックインをすることができない。

【００２８】ＥＭＤ登録サーバ３は、パーソナルコンピュータ１がＥＭＤサーバ４（４－１，４－２，４－３）からコンテンツの取得を開始するとき、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、パーソナルコンピュータ１とＥＭＤサーバ４（４－１，４－２，４－３）との相互認証に必要な認証鍵をパーソナルコンピュータ１に送信するとともに、ＥＭＤサーバ４（４－１，４－２，４－３）に接続するためのプログラムをパーソナルコンピュータ１に送信する。

【００２９】ＥＭＤサーバ４（４－１，４－２，４－３）は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、利用条件情報及びコンテンツの関連データ（例えば、曲名、又は演奏者など）とともに、パーソナルコンピュータ１にコンテンツを供給する。

【００３０】各ＥＭＤサーバ４（４－１，４－２，４－３）が配信するコンテンツは、所定の圧縮の方式で圧縮されている。その圧縮方式は、サーバ毎に異なっていてもよい。また、各ＥＭＤサーバ４（４－１，４－２，４－３）が供給するコンテンツは、所定の暗号化方式で暗号化されて配信される。その暗号化方式は、サーバ毎に異なっていてもよい。

【００３１】ＷＷＷサーバ５（５－１，５－２）は、パーソナルコンピュータ１の要求に対応して、ネットワーク２を介して、コンテンツを読み取ったＣＤ（例えば、ＣＤのアルバム名、又はＣＤの販売会社など）及びＣＤから読み取ったコンテンツに対応するデータ（例えば、曲名、又は作曲者名など）をパーソナルコンピュータ１に供給する。

【００３２】ポータブルデバイス６（６－１，６－２，６－３）は、パーソナルコンピュータ１から供給されたコンテンツ（すなわち、チェックアウトされたコンテンツ）を再生し、図示せぬヘッドフォンなどに出力する装置である。

【００３３】各ポータブルデバイス６（６－１，６－２，６－３）は、コンテンツを記憶するための記憶媒体を有している。記憶媒体としては、例えば、装置の内部基板に装着された取り外しが不可能なＩＣメモリや、着脱が可能なメモリカード等が用いられる。ポータブルデバイス６（６－１，６－２，６－３）は、ＵＳＢ等の物理的なインターフェース７（７－１，７－２，７－３）を介してパーソナルコンピュータ１と接続され、コンテンツが転送される。このとき、コンテンツは、暗号化及び圧縮された状態で転送され、利用条件情報も付加されている。

【００３４】各ポータブルデバイス６（６－１，６－２，６－３）は、通常、パーソナルコンピュータ１との接続が切り離された状態で用いられ、この状態でユーザにより再生命令が与えられると、暗号化したコンテンツを記憶媒体から読み出し、再生をする。また、各ポータブルデバイス６（６－１，６－２，６－３）は、各コンテンツに付加されている利用条件情報に基づき、また、必要に応じて再生の制限を行ったり、コンテンツの削除等の制御を行ったり、利用条件情報の更新等を行う。

【００３５】以下、ポータブルデバイス６－１，６－２，６－３を個々に区別する必要がないとき、単にポータブルデバイス６と称する。

【００３６】つぎに、図２を参照して、パーソナルコンピュータ１の構成について説明をする。

【００３７】ＣＰＵ（Central Processing Unit）１１は、各種アプリケーションプログラム（詳細については後述する。）や、ＯＳ（Operating System）を実際に実行する。ＲＯＭ（Read - only Memory）１２は、一般的には、ＣＰＵ１１が使用するプログラムや演算用

のパラメータのうちの基本的に固定のデータを格納する。ＲＡＭ（Random Access Memory）１３は、ＣＰＵ１１の実行において使用するプログラムや、その実行において適宜変化するパラメータを格納する。これらはＣＰＵバスなどから構成されるホストバス１４により相互に接続されている。

【００３８】ホストバス１４は、ブリッジ１５を介して、ＰＣＩ（Peripheral ComponentInterconnect / Interface）バスなどの外部バス１６に接続されている。

【００３９】キーボード１８は、ＣＰＵ１１に各種の指令を入力するとき、使用者により操作される。マウス１９は、ディスプレイ２０の画面上のポイントの指示や選択を行うとき、使用者により操作される。ディスプレイ２０は、液晶表示装置又はＣＲＴ（Cathode Ray Tube）などから成り、各種情報をテキストやイメージで表示する。ＨＤＤ（Hard Disk Drive）２１は、ハードディスクを駆動し、それらにＣＰＵ１１によって実行するプログラムや情報を記録又は再生させる。

【００４０】ドライブ２２は、装着されている磁気ディスク４１、光ディスク４２（ＣＤを含む）、光磁気ディスク４３、又は半導体メモリ４４に記録されているデータ又はプログラムを読み出して、そのデータ又はプログラムを、インターフェース１７、外部バス１６、ブリッジ１５及びホストバス１４を介して接続されているＲＡＭ１３に供給する。

【００４１】ＵＳＢポート２３（２３－１，２３－２，２３－３）には、ＵＳＢケーブル７（７－１，７－２，７－３）を介して、ポータブルデバイス６（６－１，６－２，６－３）が接続される。ＵＳＢポート２３は、インターフェース１７、外部バス１６、ブリッジ１５、又はホストバス１４を介して、ＨＤＤ２１、ＣＰＵ１１、又はＲＡＭ１３から供給されたデータ（例えば、コンテンツ又はポータブルデバイス６のコマンドなどを含む）をポータブルデバイス６（６－１，６－２，６－３）に出力する。

【００４２】ＩＥＣ（Internationl Electrotechnical Commission）６０９５８端子２４ａを有する音声入出力インタフェース２４は、デジタル音声入出力、あるいはアナログ音声入出力のインタフェース処理を実行する。スピーカ４５は、音声入出力インタフェース２４から供給された音声信号を基に、コンテンツに対応する所定の音声を出力する。

【００４３】これらのキーボード１８、マウス１９、ディスプレイ２０、ＨＤＤ２１、ドライブ２２、ＵＳＢポート２３、音声入出力インタフェース２４は、インターフェース１７に接続されており、インターフェース１７は、外部バス１６、ブリッジ１５及びホストバス１４を介してＣＰＵ１１に接続されている。

【００４４】通信部２５は、ネットワーク２が接続され、ＣＰＵ１１、又はＨＤＤ２１から供給されたデータ（例えば、登録の要求、又はコンテンツの送信要求など）を、所定の方式のパケットに格納して、ネットワーク２を介して、送信するとともに、ネットワーク２を介して、受信したパケットに格納されているデータ（例えば、認証鍵、又はコンテンツなど）をＣＰＵ１１、ＲＡＭ１３、又はＨＤＤ２１に出力する。

【００４５】半導体ＩＣとして、一体的に形成され、パーソナルコンピュータ１に装着されるアダプタ２６のＣＰＵ３２は、外部バス１６、ブリッジ１５及びホストバス１４を介してパーソナルコンピュータ１のＣＰＵ１１と共働し、各種の処理を実行する。ＲＡＭ３３は、ＣＰＵ３２が各種の処理を実行する上において必要なデータやプログラムを記憶する。不揮発性メモリ３４は、パーソナルコンピュータ１の電源がオフされた後も保持する必要があるデータを記憶する。ＲＯＭ３６には、パーソナルコンピュータ１から、暗号化されているプログラムが転送されてきたとき、それを復号するプログラムが記憶されている。ＲＴＣ（Real Time Clock）３５は、計時動作を実行し、時刻情報を提供する。半導体ＩＣは、セキュアな環境に設計されており、外部からの悪意なアクセスに対して耐性をもっている。なお、この機能は、ソフトウェアプログラムで構成されていてもよい。

【００４６】通信部２５及びアダプタ２６は、外部バス１６、ブリッジ１５及びホストバス１４を介してＣＰＵ１１に接続されている。

【００４７】次に、図３を参照して、ポータブルデバイス６の構成を説明する。

【００４８】電源回路５２は、乾電池５１から供給される電源電圧を所定の電圧の内部電力に変換して、ＣＰＵ５３～表示部６７に供給することにより、ポータブルデバイス６全体を駆動させる。

【００４９】ＵＳＢコントローラ５７は、ＵＳＢコネクタ５６を介して、パーソナルコンピュータ１とＵＳＢケーブル７を介して接続された場合、パーソナルコンピュータ１から転送されたコンテンツを含むデータを、内部バス５８を介して、ＣＰＵ５３に供給する。

【００５０】パーソナルコンピュータ１から転送されるデータは、１パケット当たり６４バイトのデータから構成され、１２Ｍｂｉｔ／ｓｅｃの転送レートでパーソナルコンピュータ１から転送される。

【００５１】ポータブルデバイス６に転送されるデータは、ヘッダ及びコンテンツから構成される。ヘッダには、コンテンツＩＤ、ファイル名、ヘッダサイズ、コンテンツ鍵、ファイルサイズ、コーデックＩＤ、ファイル情報などが格納されているとともに、再生制限処理等に必要な利用条件情報等が格納されている。コンテンツは、ＡＴＲＡＣ３などの符号化方式で符号化され、暗号化されている。

【００５２】ヘッダサイズは、ヘッダのデータ長（例え

ば、３３バイトなど）を表し、ファイルサイズは、コンテンツのデータ長（例えば、３３，６３６，１３８バイトなど）を表す。

【００５３】コンテンツ鍵は、暗号化されているコンテンツを復号するための鍵であり、パーソナルコンピュータ１とポータブルデバイス６との相互認証の処理で生成されたセッション鍵（一時鍵）を基に暗号化された状態で、パーソナルコンピュータ１からポータブルデバイス６に送信される。

【００５４】ポータブルデバイス６がＵＳＢケーブル７を介してパーソナルコンピュータ１のＵＳＢポート２３に接続されたとき、ポータブルデバイス６とパーソナルコンピュータ１とは、相互認証の処理を実行する。この相互認証の処理は、例えば、チャレンジレスポンス方式の認証の処理である。ちなみに、ポータブルデバイス６のＤＳＰ５９は、チャレンジレスポンス方式の認証の処理を行うとき、暗号解読（復号）の処理を実行する。

【００５５】チャレンジレスポンス方式とは、例えば、パーソナルコンピュータ１が生成するある値（チャレンジ）に対して、ポータブルデバイス６がパーソナルコンピュータ１と共有している秘密鍵を使用して生成した値（レスポンス）で応答する方式である。チャレンジレスポンス方式の相互認証の処理においては、パーソナルコンピュータ１が生成する値は認証の処理毎に毎回変化するので、例えば、ポータブルデバイス６が出力した、秘密鍵を使用して生成された値が読み出されて、いわゆる、なりすましの攻撃を受けても、次の相互認証の処理では、相互認証に使用される値が異なるので、パーソナルコンピュータ１は不正を検出できる。

【００５６】コンテンツＩＤは、コンテンツに対応した、コンテンツを特定するためのＩＤである。

【００５７】コーデックＩＤは、コンテンツの符号化方式に対応したＩＤであり、例えば、コーデックＩＤ”１”は、ＡＴＲＡＣ３に対応し、コーデックＩＤ”０”は、ＭＰ３（MPEG（Moving Picture Experts Group） Audio Layer-3）に対応する。

【００５８】ファイル名は、コンテンツに対応するパーソナルコンピュータ１が記録しているコンテンツファイル（後述する）をＡＳＣＩＩ（American National Standard Code for Information Interchange）コードに変換したデータであり、ファイル情報は、コンテンツに対応する曲名、アーティスト名、作詞者名、又は作曲者名などをＡＳＣＩＩコードに変換したデータである。

【００５９】ポータブルデバイス６が、パーソナルコンピュータ１からコンテンツとともにコンテンツの書き込み命令を受信した場合、ＲＡＭ５４又はＲＯＭ５５から読み出したメインプログラムを実行するＣＰＵ５３は、書き込み命令を受け取り、フラッシュメモリコントローラ６０を制御して、パーソナルコンピュータ１から受信したコンテンツをフラッシュメモリ６１に書き込ませる。

【００６０】フラッシュメモリ６１は、約６４ＭＢｙｔｅの記憶容量を有し、コンテンツを記憶する。また、フラッシュメモリ６１には、所定の圧縮方式で圧縮されているコンテンツを伸張するための再生用コードが予め格納されている。

【００６１】なお、フラッシュメモリ６１は、ポータブルデバイス６にメモリカードとして着脱可能とすることができるようにしてもよい。

【００６２】使用者による、図示せぬ再生／停止ボタンの押し下げ操作に対応した再生命令が操作キーコントローラ６２を介してＣＰＵ５３に供給されると、ＣＰＵ５３は、フラッシュメモリコントローラ６０に、フラッシュメモリ６１から、再生用コードとコンテンツとを読み出させ、ＤＳＰ５９に転送させる。

【００６３】ＤＳＰ５９は、フラッシュメモリ６１から転送された再生用コードに基づいてコンテンツをＣＲＣ（Cyclic Redundancy Check）方式で誤り検出をした後、再生して、再生したデータ（図３中においてＤ１で示す）をディジタル／アナログ変換回路６３に供給する。

【００６４】ＤＳＰ５９は、内部に設けられた発信回路とともに一体に構成され、外付けされた水晶で成る発信子５９ＡからのマスタークロックＭＣＬＫを基に、コンテンツを再生するとともに、マスタークロックＭＣＬＫ、マスタークロックＭＣＬＫを基に内部の発振回路で生成した所定の周波数のビットクロックＢＣＬＫ、並びに、フレーム単位のＬチャンネルクロックＬＣＬＫ及びＲチャンネルクロックＲＣＬＫからなる動作クロックＬＲＣＬＫをディジタルアナログ変換回路６３に供給する。

【００６５】ＤＳＰ５９は、コンテンツを再生するとき、再生用コードに従って上述の動作クロックをディジタルアナログ変換回路６３に供給して、コンテンツを再生しないとき、再生用コードに従って動作クロックの供給を停止して、ディジタルアナログ変換回路６３を停止させて、ポータブルデバイス６全体の消費電力量を低減する。

【００６６】同様に、ＣＰＵ５３及びＵＳＢコントローラ５７も、水晶でなる発振子５３Ａ又は５７Ａがそれぞれ外付けされ、発振子５３Ａ又は５７Ａからそれぞれ供給されるマスタークロックＭＣＬＫに基づき、所定の処理を実行する。

【００６７】このように構成することで、ポータブルデバイス６は、ＣＰＵ５３，ＤＳＰ５９，ＵＳＢコントローラ５７等の各回路ブロックに対してクロック供給を行うためのクロック発生モジュールが不要となり、回路構成を簡素化するとともに小型化することができる。

【００６８】ディジタルアナログ変換回路６３は、再生したコンテンツをアナログの音声信号に変換して、これ

を増幅回路６４に供給する。増幅回路６４は、音声信号を増幅して、ヘッドフォンジャック６５を介して、ヘッドフォンに音声信号を供給する。

【００６９】このように、ポータブルデバイス６は、再生／停止ボタンが押圧操作されたとき、ＣＰＵ５３の制御に基づいてフラッシュメモリ６１に記憶されているコンテンツを再生するとともに、再生中に再生／停止ボタンが押圧操作されたとき、コンテンツの再生を停止する。

【００７０】ポータブルデバイス６は、停止後に再度再生／停止ボタンが押圧操作されたとき、ＣＰＵ５３の制御に基づいて停止した位置からコンテンツの再生を再開する。再生／停止ボタンが押圧操作により再生を停止して操作が加わることなく数秒間経過したとき、ポータブルデバイス６は、自動的に電源をオフして消費電力を低減する。

【００７１】因みに、ポータブルデバイス６は、電源がオフになった後に再生／停止ボタンが押圧操作されたとき、前回の停止した位置からコンテンツを再生せず、１曲目から再生する。

【００７２】また、ポータブルデバイス６のＣＰＵ５３は、ＬＣＤコントローラ６８を制御して、表示部６７に、再生モードの状態（例えば、リピート再生、イントロ再生など）、イコライザ調整（すなわち、音声信号の周波数帯域に対応した利得の調整）、曲番号、演奏時間、再生、停止、早送り、早戻しなどの状態、音量及び乾電池５１の残量等の情報を表示させる。

【００７３】さらに、ポータブルデバイス６は、ＥＥＰＲＯＭ６８に、フラッシュメモリ８０に書き込まれているコンテンツの数、それぞれのコンテンツが書き込まれているフラッシュメモリ６１のブロック位置及びその他種々のメモリ蓄積情報等のいわゆるＦＡＴ（ File Allocation Table ）を格納する。

【００７４】因みに、本実施の形態においては、コンテンツは、６４ＫＢｙｔｅを１ブロックとして扱われ、１曲のコンテンツに対応したブロック位置がＦＡＴに格納される。

【００７５】フラッシュメモリ６１にＦＡＴが格納される場合、例えば、１曲目のコンテンツがＣＰＵ５３の制御によりフラッシュメモリ６１に書き込まれると、１曲目のコンテンツに対応するブロック位置がＦＡＴとしてフラッシュメモリ６１に書き込まれ、次に、２曲目のコンテンツがフラッシュメモリ６１に書き込まれると、２曲目のコンテンツに対応するブロック位置がＦＡＴとしてフラッシュメモリ６１（１曲目と同一の領域）に書き込まれる。

【００７６】このように、ＦＡＴは、フラッシュメモリ６１へのコンテンツの書き込みのたびに書き換えられ、更に、データの保護の為、同一のデータがリザーブ用に２重に書き込まれる。

【００７７】ＦＡＴがフラッシュメモリ６１に書き込まれると、１回のコンテンツの書き込みに対応して、フラッシュメモリ６１の同一の領域が２回書き換えられるので、少ないコンテンツの書き込みの回数で、フラッシュメモリ６１に規定されている書換えの回数に達してしまい、フラッシュメモリ６１の書換えができなくなってしまう。

【００７８】そこで、ポータブルデバイス６は、ＦＡＴをＥＥＰＲＯＭ６８に記憶させて、１回のコンテンツの書き込みに対応するフラッシュメモリ６１の書換えの頻度を少なくしている。

【００７９】書換えの回数の多いＦＡＴをＥＥＰＲＯＭ６８に記憶させることにより、ＦＡＴをフラッシュメモリ６１に記憶させる場合に比較して、ポータブルデバイス６は、コンテンツの書き込みができる回数を数十倍以上に増やすことができる。更に、ＣＰＵ５３は、ＥＥＰＲＯＭ６８にＦＡＴを追記するように書き込ませるので、ＥＥＰＲＯＭ６８の同一の領域の書換えの頻度を少なくして、ＥＥＰＲＯＭ６８が短期間で書換え不能になることを防止する。

【００８０】ポータブルデバイス６は、ＵＳＢケーブル７を介してパーソナルコンピュータ１に接続されたとき（以下、これをＵＳＢ接続と称する）、ＵＳＢコントローラ５７からＣＰＵ５３に供給される割り込み信号に基づき、ＵＳＢ接続されたことを認識する。

【００８１】ポータブルデバイス６は、ＵＳＢ接続されたことを認識すると、パーソナルコンピュータ１からＵＳＢケーブル７を介して規定電流値の外部電力の供給を受けるとともに、電源回路５２を制御して、乾電池５１からの電力の供給を停止させる。

【００８２】ＣＰＵ５３は、ＵＳＢ接続されたとき、ＤＳＰ５９のコンテンツの再生の処理を停止させる。これにより、ＣＰＵ５３は、パーソナルコンピュータ１から供給される外部電力が規定電流値を超えてしまうことを防止して、規定電流値の外部電力を常時受けられるように制御する。

【００８３】このようにＣＰＵ５３は、ＵＳＢ接続されると、乾電池５１から供給される電力からパーソナルコンピュータ１から供給される電力に切り換えるので、電力単価の安いパーソナルコンピュータ１からの外部電力が使用され、電力単価の高い乾電池５１の消費電力が低減され、かくして乾電池５１の寿命を延ばすことができる。

【００８４】なお、ＣＰＵ５３は、パーソナルコンピュータ１からＵＳＢケーブル７を介して外部電力の供給を受けたとき、ＤＳＰ５９の再生処理を停止させることにより、ＤＳＰ５９からの輻射を低減させ、その結果としてパーソナルコンピュータ１を含むシステム全体の輻射を一段と低減させる。

【００８５】つぎに、パーソナルコンピュータ１にイン

ストールされたプログラムの実行等により実現されるパーソナルコンピュータ１の機能について説明する。

【００８６】図４は、所定のプログラムの実行等により実現される、パーソナルコンピュータ１の機能の構成を示す図である。

【００８７】コンテンツ管理プログラム１１１は、ＥＭＤ選択プログラム１３１、チェックイン／チェックアウト管理プログラム１３２、コピー管理プログラム１３３、移動管理プログラム１３４、暗号方式変換プログラム１３５、圧縮方式変換プログラム１３６、暗号化プログラム１３７、利用条件変換プログラム１３９、利用条件管理プログラム１４０、認証プログラム１４１、復号プログラム１４２、ＰＤ用ドライバ１４３、購入用プログラム１４４及び購入用プログラム１４５などの複数のプログラムで構成されている。

【００８８】コンテンツ管理プログラム１１１は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、コンテンツ管理プログラム１１１を読み出しても、インストラクションを特定できないなど）ように構成されている。

【００８９】ＥＭＤ選択プログラム１３１は、コンテンツ管理プログラム１１１がパーソナルコンピュータ１にインストールされるとき、コンテンツ管理プログラム１１１には含まれず、ＥＭＤの登録の際に、ネットワーク２を介して、ＥＭＤ登録サーバ３から受信される。ＥＭＤ選択プログラム１３１は、ＥＭＤサーバ４（４－１，４－２，４－３）のとの接続を選択して、購入用アプリケーション１１５、又は購入用プログラム１４４，１４５に、ＥＭＤサーバ４（４－１，４－２，４－３）との通信（例えば、コンテンツを購入するときの、コンテンツのダウンロードなど）を実行させる。

【００９０】チェックイン／チェックアウト管理プログラム１３２は、チェックイン又はチェックアウトの設定、及びコンテンツデータベース１１４に記録されている利用条件ファイル１６２－１～１６２－Ｎに基づいて、コンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツをポータブルデバイス６にチェックアウトするか、又はポータブルデバイス６に記憶されているコンテンツをチェックインする。

【００９１】チェックイン／チェックアウト管理プログラム１３２は、チェックイン又はチェックアウトの処理に対応して、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１～１６２－Ｎに格納されている利用条件情報を更新する。

【００９２】コピー管理プログラム１３３は、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１～１６２－Ｎに基づいて、コンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツをポータブルデバイス６にコピーするか、又はポータブルデバイス６からコンテンツをコンテンツデータベース１１４にコピーする。

【００９３】移動管理プログラム１３４は、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１～１６２－Ｎに基づいて、コンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツをポータブルデバイス６に移動するか、又はポータブルデバイス６からコンテンツをコンテンツデータベース１１４に移動する。

【００９４】暗号方式変換プログラム１３５は、ネットワーク２を介して、購入用アプリケーションプログラム１１５がＥＭＤサーバ４－１から受信したコンテンツの暗号化の方式、購入用プログラム１４４がＥＭＤサーバ４－２から受信したコンテンツの暗号化の方式を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツと同一の暗号化の方式に変換する。

【００９５】圧縮方式変換プログラム１３６は、ネットワーク２を介して、購入用アプリケーションプログラム１１５がＥＭＤサーバ４－１から受信したコンテンツの圧縮の方式、購入用プログラム１４４がＥＭＤサーバ４－２から受信したコンテンツの圧縮の方式を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツと同一の圧縮の方式に変換する。

【００９６】暗号化プログラム１３７は、例えばＣＤから読み取られ、録音プログラム１１３から供給されたコンテンツ（暗号化されていない）を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツと同一の暗号化の方式で暗号化する。

【００９７】圧縮／伸張プログラム１３８は、例えばＣＤから読み取られ、録音プログラム１１３から供給されたコンテンツ（圧縮されていない）を、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツと同一の符号化の方式で符号化する。圧縮／伸張プログラム１３８は、符号化されているコンテンツを伸張（復号）する。

【００９８】利用条件変換プログラム１３９は、ネットワーク２を介して、購入用アプリケーションプログラム１１５がＥＭＤサーバ４－１から受信したコンテンツの利用条件情報（いわゆる、Ｕｓａｇｅ　Ｒｕｌｅ）、購入用プログラム１４４がＥＭＤサーバ４－２から受信したコンテンツの利用条件情報を、コンテンツデータベース１１４が記録している利用条件ファイル１６２－１～１６２－Ｎに格納されている利用条件情報と同一のフォーマットに変換する。

【００９９】利用条件管理プログラム１４０は、コンテ

ンツのコピー、移動、チェックイン、又はチェックアウトの処理を実行する前に、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１～１６２－Ｎに格納されている利用条件情報に対応するハッシュ値を基に、利用条件情報の改竄を検出する。利用条件管理プログラム１４０は、コンテンツのコピー、移動、チェックイン、又はチェックアウトの処理に伴う、コンテンツデータベース１１４に記録されている利用条件ファイル１６２－１～１６２－Ｎに格納されている利用条件情報を更新に対応して、利用条件情報に対応するハッシュ値を更新する。

【０１００】認証プログラム１４１は、コンテンツ管理プログラム１１１と購入用アプリケーションプログラム１１５との相互認証の処理及びコンテンツ管理プログラム１１１と購入用プログラム１４４との相互認証の処理を実行する。また、認証プログラム１４１は、ＥＭＤサーバ４－３と購入用プログラム１４５との相互認証の処理で利用される認証鍵を記憶している。

【０１０１】認証プログラム１４１が相互認証の処理で利用する認証鍵は、コンテンツ管理プログラム１１１がパーソナルコンピュータ１にインストールされたとき、認証プログラム１４１に記憶されておらず、表示操作指示プログラム１１２により登録の処理が正常に実行されたとき、ＥＭＤ登録サーバ３から供給され、認証プログラム１４１に記憶される。

【０１０２】復号プログラム１４２は、コンテンツデータベース１１４が記録しているコンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツをパーソナルコンピュータ１が再生するとき、コンテンツを復号する。

【０１０３】ＰＤ用ドライバ１４３は、ポータブルデバイス６に所定のコンテンツをチェックアウトするとき、又はポータブルデバイスから所定のコンテンツをチェックインするとき、ポータブルデバイス６にコンテンツ又はポータブルデバイス６に所定の処理を実行させるコマンドを供給する。

【０１０４】購入用プログラム１４４は、コンテンツ管理プログラム１１１とともにインストールされ、ＥＭＤ登録サーバ３からネットワーク２を介して供給され、又は所定のＣＤに記録されて供給される。購入用プログラム１４４は、パーソナルコンピュータ１にインストールされたとき、コンテンツ管理プログラム１１１の有する所定の形式のインターフェースを介して、コンテンツ管理プログラム１１１とデータを送受信する。

【０１０５】購入用プログラム１４４は、例えば、シャッフルされているインストラクション、又は暗号化されているインストラクションなどで記述されて、その処理内容を外部から隠蔽し、その処理内容の読解が困難になる（例えば、使用者が、直接、購入用プログラム１４４を読み出しても、インストラクションを特定できないなど）ように構成されている。

【０１０６】購入用プログラム１４４は、ネットワーク２を介して、ＥＭＤサーバ４－２に所定のコンテンツの送信を要求するとともに、ＥＭＤサーバ４－２からコンテンツを受信する。また、購入用プログラム１４４は、ＥＭＤサーバ４－２からコンテンツを受信するとき、課金の処理を実行する。

【０１０７】購入用プログラム１４５は、コンテンツ管理プログラム１１１とともにインストールされるプログラムであり、ネットワーク２を介して、ＥＭＤサーバ４－３に所定のコンテンツの送信を要求するとともに、ＥＭＤサーバ４－３からコンテンツを受信する。また、購入用プログラム１４５は、ＥＭＤサーバ４－３からコンテンツを受信するとき、課金の処理を実行する。

【０１０８】表示操作指示プログラム１１２は、フィルタリングデータファイル１８１、表示データファイル１８２、画像ファイル１８３－１～１８３－Ｋ、又は履歴データファイル１８４を基に、ディスプレイ２０に所定のウィンドウの画像を表示させ、キーボード１８又はマウス１９への操作を基に、コンテンツ管理プログラム１１１にチェックイン又はチェックアウトなどの処理の実行を指示する。

【０１０９】フィルタリングデータファイル１８１は、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツそれぞれに重み付けをするためのデータを格納して、ＨＤＤ２１に記録されている。

【０１１０】表示データファイル１８２は、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツに対応するデータを格納して、ＨＤＤ２１に記録されている。

【０１１１】画像ファイル１８３－１～１８３－Ｋは、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１～１６１－Ｎに対応する画像、又は後述するパッケージに対応する画像を格納して、ＨＤＤ２１に記録されている。

【０１１２】以下、画像ファイル１８３－１～１８３－Ｋを個々に区別する必要がないとき、単に、画像ファイル１８３と称する。

【０１１３】履歴データファイル１８４は、コンテンツデータベース１１４に記録されているコンテンツファイル１６１－１～１６１－Ｎに格納されているコンテンツがチェックアウトされた回数、チェックインされた回数、その日付などの履歴データを格納して、ＨＤＤ２１に記録されている。

【０１１４】表示操作指示プログラム１１２は、登録の処理のとき、ネットワーク２を介して、ＥＭＤ登録サーバ３に、予め記憶しているコンテンツ管理プログラム１１１のＩＤを送信するとともに、ＥＭＤ登録サーバ３か

ら認証用鍵及びＥＭＤ選択プログラム１３１を受信して、コンテンツ管理プログラム１１１に認証用鍵及びＥＭＤ選択プログラム１３１を供給する。

【０１１５】録音プログラム１１３は、所定のウィンドウの画像を表示させて、キーボード１８又はマウス１９への操作を基に、ドライブ２２に装着された光ディスク４２であるＣＤからコンテンツの録音時間などのデータを読み出す。

【０１１６】録音プログラム１１３は、ＣＤに記録されているコンテンツの録音時間などを基に、ネットワーク２を介して、WWWサーバ５－１又は５－２にＣＤに対応するデータ（例えば、アルバム名、又はアーティスト名など）又はＣＤに記録されているコンテンツに対応するデータ（例えば、曲名など）の送信を要求するとともに、WWWサーバ５－１又は５－２からＣＤに対応するデータ又はＣＤに記録されているコンテンツに対応するデータを受信する。

【０１１７】録音プログラム１１３は、受信したＣＤに対応するデータ又はＣＤに記録されているコンテンツに対応するデータを、表示操作指示プログラム１１２に供給する。

【０１１８】また、録音の指示が入力されたとき、録音プログラム１１３は、ドライブ２２に装着された光ディスク４２であるＣＤからコンテンツを読み出して、コンテンツ管理プログラム１１１に出力する。

【０１１９】コンテンツデータベース１１４は、コンテンツ管理プログラム１１１から供給された所定の方式で圧縮され、所定の方式で暗号化されているコンテンツを、コンテンツファイル１６１－１～１６１－Ｎのいずれかに格納する（ＨＤＤ２１に記録する）。コンテンツデータベース１１４は、コンテンツファイル１６１－１～１６１－Ｎにそれぞれ格納されているコンテンツに対応する利用条件情報を、コンテンツが格納されているコンテンツファイル１６１－１～１６１－Ｎにそれぞれ対応する利用条件ファイル１６２－１～１６２－Ｎのいずれかに格納する（ＨＤＤ２１に記録する）。

【０１２０】コンテンツデータベース１１４は、コンテンツファイル１６１－１～１６１－Ｎ又は利用条件ファイル１６２－１～１６２－Ｎをレコードとして記録してもよい。

【０１２１】例えば、コンテンツファイル１６１－１に格納されているコンテンツに対応する利用条件情報は、利用条件ファイル１６２－１に格納されている。コンテンツファイル１６１－Ｎに格納されているコンテンツに対応する利用条件情報は、利用条件ファイル１６２－Ｎに格納されている。

【０１２２】以下、コンテンツファイル１６１－１～１６１－Ｎを個々に区別する必要がないとき、単に、コンテンツファイル１６１と称する。以下、利用条件ファイル１６２－１～１６２－Ｎを個々に区別する必要がないとき、単に、利用条件ファイル１６２と称する。

【０１２３】購入用アプリケーションプログラム１１５は、ＥＭＤ登録サーバ３からネットワーク２を介して供給され、又は所定のＣＤ－ＲＯＭに記録されて供給される。購入用アプリケーションプログラム１１５は、ネットワーク２を介して、ＥＭＤサーバ４－１に所定のコンテンツの送信を要求するとともに、ＥＭＤサーバ４－１からコンテンツを受信して、コンテンツ管理プログラム１１１に供給する。また、購入用アプリケーションプログラム１１５は、ＥＭＤサーバ４－１からコンテンツを受信するとき、課金の処理を実行する。

【０１２４】次に、表示データファイル１８２に格納されているデータとコンテンツデータベースに格納されているコンテンツファイル１６１－１～１６１－Ｎとの対応付けについて説明する。

【０１２５】コンテンツファイル１６１－１～１６１－Ｎのいずれかに格納されているコンテンツは、所定のパッケージに属する。パッケージは、より詳細には、オリジナルパッケージ、マイセレクトパッケージ、又はフィルタリングパッケージのいずれかである。

【０１２６】オリジナルパッケージは、１以上のコンテンツが属し、ＥＭＤサーバ４におけるコンテンツの分類（例えば、いわゆるアルバムに対応する）、又は一枚のＣＤに対応する。コンテンツは、いずれかのオリジナルパッケージに属し、複数のオリジナルパッケージに属することができない。また、コンテンツが属するオリジナルパッケージは、変更することができない。使用者は、オリジナルパッケージに対応する情報の一部を編集（情報の追加、又は追加した情報の変更）することができる。

【０１２７】マイセレクトパッケージは、使用者が任意に選択した１以上のコンテンツが属する。マイセレクトパッケージにいずれのコンテンツが属するかは、使用者が任意に編集することができる。コンテンツは、１以上のマイセレクトパッケージに同時に属することができる。また、コンテンツは、いずれのマイセレクトパッケージに属しなくともよい。

【０１２８】フィルタリングパッケージには、フィルタリングデータファイル１８１に格納されているフィルタリングデータを基に選択されたコンテンツが属する。フィルタリングデータは、ＥＭＤサーバ４又はWWWサーバ５などからネットワーク２を介して供給され、又は所定のＣＤに記録されて供給される。使用者は、フィルタリングデータファイル１８１に格納されているフィルタリングデータを編集することができる。

【０１２９】フィルタリングデータは、所定のコンテンツを選択する、又はコンテンツに対応する重みを算出する基準となる。例えば、今週のＪ－ＰＯＰ（日本のポップス）ベストテンに対応するフィルタリングデータを利用すれば、パーソナルコンピュータ１は、今週の日本の

ポップス１位のコンテンツ～今週の日本のポップス１０位のコンテンツを特定することができる。

【０１３０】フィルタリングデータファイル１８１は、例えば、過去１月間にチェックアウトされていた期間が長い順にコンテンツを選択するフィルタリングデータ、過去半年間にチェックアウトされた回数が多いコンテンツを選択するフィルタリングデータ、又は曲名に”愛”の文字が含まれているコンテンツを選択するフィルタリングデータなどを含んでいる。

【０１３１】このようにフィルタリングパッケージのコンテンツは、コンテンツに対応するコンテンツ用表示データ２２１（コンテンツ用表示データ２２１に使用者が設定したデータを含む）、又は履歴データ１８４などと、フィルタリングデータとを対応させて選択される。

【０１３２】ドライバ１１７は、コンテンツ管理プログラム１１１などの制御の基に、音声入出力インターフェース２４を駆動して、外部から供給されたデジタルデータであるコンテンツを入力してコンテンツ管理プログラム１１１に供給するか、若しくはコンテンツ管理プログラム１１１を介してコンテンツデータベース１１４から供給されたコンテンツをデジタルデータとして出力するか、又は、コンテンツ管理プログラム１１１を介してコンテンツデータベース１１４から供給されたコンテンツに対応するアナログ信号を出力する。

【０１３３】図５は、表示操作指示プログラム１１２を起動させたとき、操作指示プログラム１１２がディスプレイ２０に表示させる表示操作指示ウィンドウの例を示す図である。

【０１３４】表示操作指示ウィンドウには、録音プログラム１１３を起動させるためのボタン２０１、ＥＭＤ選択プログラム１３１を起動させるためのボタン２０２、チェックイン又はチェックアウトの処理の設定を行うフィールドを表示させるためのボタン２０３、マイセレクトパッケージを編集するためフィールドを表示させるためのボタン２０４等が配置されている。

【０１３５】ボタン２０５が選択されているとき、フィールド２１１には、オリジナルパッケージに対応するデータが表示される。ボタン２０６が選択されているとき、フィールド２１１には、マイセレクトパッケージに対応するデータが表示される。ボタン２０７が選択されているとき、フィールド２１１には、フィルタリングパッケージに対応するデータが表示される。

【０１３６】フィールド２１１に表示されるデータは、パッケージに関するデータであり、例えば、パッケージ名称、又はアーティスト名などである。

【０１３７】例えば、図５においては、パッケージ名称”ファースト”及びアーティスト名”Ａ太郎”、パッケージ名称”セカンド”及びアーティスト名”Ａ太郎”などがフィールド２１１に表示される。

【０１３８】フィールド２１２には、フィールド２１１で選択されているパッケージに属するコンテンツに対応するデータが表示される。フィールド２１２に表示されるデータは、例えば、曲名、演奏時間、又はチェックアウト可能回数などである。

【０１３９】例えば、図５においては、パッケージ名称”セカンド”に対応するパッケージが選択されているので、パッケージ名称”セカンド”に対応するパッケージに属するコンテンツに対応する曲名”南の酒場”及びチェックアウト可能回数（例えば、８分音符の１つがチェックアウト１回に相当し、８分音符が２つでチェックアウト２回を示す）、並びに曲名”北の墓場”及びチェックアウト可能回数（８分音符が１つでチェックアウト１回を示す）などがフィールド２１２に表示される。

【０１４０】このように、フィールド２１２に表示されるチェックアウト可能回数としての１つの８分音符は、対応するコンテンツが１回チェックアウトできることを示す。

【０１４１】フィールド２１２に表示されるチェックアウト可能回数としての休符は、対応するコンテンツがチェックアウトできない（チェックアウト可能回数が０である。（ただし、パーソナルコンピュータ１はそのコンテンツを再生することができる。））ことを示す。また、フィールド２１２に表示されるチェックアウト可能回数としてのト音記号は、対応するコンテンツのチェックアウトの回数に制限がない（何度でも、チェックアウトできる）ことを示している。

【０１４２】なお、チェックアウト可能回数は、図５に示すように所定の図形（例えば、円、星、月などでもよい）の数で表示するだけでなく、数字等で表示してもよい。

【０１４３】また、表示操作指示ウィンドウには、選択されているパッケージ又はコンテンツに対応付けられている画像等（図４の画像ファイル１８３－１～１８３－Ｋのいずれかに対応する）を表示させるフィールド２０８が配置されている。ボタン２０９は、選択されているコンテンツを再生する（コンテンツに対応する音声をスピーカ４５に出力させる）とき、クリックされる。

【０１４４】ボタン２０５が選択され、フィールド２１１に、オリジナルパッケージに対応するデータが表示されている場合、フィールド２１２に表示されている所定のコンテンツの曲名を選択して、消去の操作をしたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１に、選択されている曲名に対応する、コンテンツデータベース１１４に格納されている所定のコンテンツを消去させる。

【０１４５】録音プログラム１１３が表示させるウィンドウのボタン（後述するボタン２５５）が選択されて（アクティブにされて）いる場合、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、表示操作指示プログラム１１２は、表示操作指

示ウィンドウに、予め指定されているポータブルデバイス６に記憶されているコンテンツの曲名を表示するフィールド２１３を表示する。

【０１４６】録音プログラム１１３が表示させるウィンドウのボタンが選択されている場合、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１に、コンテンツデータベース１１４に記録した、ＣＤから読み出したコンテンツを予め指定されているポータブルデバイス６にチェックアウトさせる。

【０１４７】フィールド２１３にはコンテンツの曲名に対応させて、フィールド２１３の最も左に、そのコンテンツがパーソナルコンピュータ１にチェックインできるか否かを示す記号が表示される。例えば、フィールド２１３の最も左に位置する“○”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ１にチェックインできる（すなわち、パーソナルコンピュータ１からチェックアウトされた）ことを示している。フィールド２１３の最も左に位置する“×”は、コンテンツの曲名に対応するコンテンツがパーソナルコンピュータ１にチェックインできない（すなわち、パーソナルコンピュータ１からチェックアウトされていない、例えば、他のパーソナルコンピュータからチェックアウトされた）ことを示している。

【０１４８】表示操作指示プログラム１１２が表示操作指示ウィンドウにフィールド２１３を表示させたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、予め指定されているポータブルデバイス６に記憶されているコンテンツが属するポータブルパッケージ（ポータブルデバイス６に記憶されているコンテンツが属するパーケージ）の名称を表示するフィールド２１４、フィールド２１３を閉じるためのボタン２１０及びチェックイン又はチェックアウトを実行させるボタン２１５を表示する。

【０１４９】更に、表示操作指示プログラム１１２が表示操作指示ウィンドウにフィールド２１３を表示させたとき、表示操作指示プログラム１１２は、表示操作指示ウィンドウに、フィールド２１２で選択された曲名に対応するコンテンツのチェックアウトを設定するボタン２１６、フィールド２１３で選択された曲名に対応するコンテンツのチェックインを設定するボタン２１７、フィールド２１３に表示されたコンテンツ名に対応する全てのコンテンツのチェックインを設定するボタン２１８及びチェックイン又はチェックアウトの設定を取り消すボタン２１９を配置させる。

【０１５０】ボタン２１６乃至２１９の操作によるチェックイン又はチェックアウトの設定だけでは、パーソナルコンピュータ１は、チェックイン又はチェックアウトの処理を実行しない。

【０１５１】ボタン２１６乃至２１９の操作によるチェックイン又はチェックアウトの設定をした後、ボタン２１５がクリックされたとき、表示操作指示プログラム１１２は、コンテンツ管理プログラム１１１にチェックイン又はチェックアウトの処理を実行させる。すなわち、ボタン２１５がクリックされたとき、表示操作指示プログラム１１２は、チェックイン又はチェックアウトの設定に基づき、コンテンツ管理プログラム１１１に、ポータブルデバイス６にコンテンツを送信させるか、又はチェックインに対応する所定のコマンド（例えば、ポータブルデバイス６が記憶している所定のコンテンツを消去させるコマンドなど）を送信させるとともに、送信したコンテンツ又はコマンドに対応する利用条件ファイル１６２に格納されている利用条件情報を更新させる。

【０１５２】チェックイン又はチェックアウトが実行されたとき、表示操作指示プログラム１１２は、送信したコンテンツ又は送信されたコマンドに対応して、履歴データファイル１８４に格納されている履歴データを更新する。履歴データは、チェックイン又はチェックアウトされたコンテンツを特定する情報、又はそのコンテンツがチェックイン又はチェックアウトされた日付、そのコンテンツがチェックアウトされたポータブルデバイス６の名称などから成る。

【０１５３】チェックイン又はチェックアウトの設定の処理は短時間で実行できるので、使用者は、チェックイン又はチェックアウトの処理の実行後の状態を迅速に知ることができ、時間のかかるチェックイン又はチェックアウトの処理の回数を減らして、チェックイン又はチェックアウトに必要な時間全体（設定及び実行を含む）を短くすることができる。

【０１５４】図６は、録音プログラム１１３がディスプレイ２０に表示させるウィンドウの例を説明する図である。

【０１５５】例えば、WWWサーバ５－２から受信したＣＤの情報を基に、録音プログラム１１３は、フィールド２５１に、”アシンクロナイズド”などのＣＤのタイトルを表示する。WWWサーバ５－２から受信したＣＤの情報を基に、録音プログラム１１３は、フィールド２５２に、例えば、”クワイ”などのアーティスト名を表示する。

【０１５６】WWWサーバ５－２から受信したＣＤの情報を基に、録音プログラム１１３は、フィールド２５３の曲名を表示する部分に、例えば、”ヒート”，”プラネット”，”ブラック”，”ソウル”などの曲名を表示する。同様に、録音プログラム１１３は、フィールド２５３のアーティストを表示する部分に、例えば、”クワイ”などのアーティスト名を表示する。

【０１５７】録音プログラム１１３が所定のＣＤの情報を受信した後、録音プログラム１１３は、ＨＤＤ２１の所定のディレクトリにＣＤの情報を格納する。

【０１５８】ボタン２５４などがクリックされて、ＣＤの情報の取得の指示を受けたとき、録音プログラム１１３は、始めに、ＨＤＤ２１の所定のディレクトリを検索する。録音プログラム１１３は、そのディレクトリにＣＤの情報が格納されているとき、図示せぬダイアログボックスを表示して、使用者にディレクトリに格納されているＣＤの情報を利用するか否かを選択させる。

【０１５９】録音プログラム１１３が表示させるウィンドウに配置されているコンテンツの録音の開始を指示するボタン２５６がクリックされたとき、録音プログラム１１３は、ドライブ２２に格納されているＣＤからコンテンツを読み出して、ＣＤから読み出したコンテンツをＣＤの情報とともにコンテンツ管理プログラム１１１に供給する。コンテンツ管理プログラム１１１の圧縮／伸張プログラム１３８は、録音プログラム１１３から供給されたコンテンツを所定の圧縮の方式で圧縮して、暗号化プログラム１３７は、圧縮されたコンテンツを、暗号化する。また、利用条件変換プログラム１３９は、圧縮され、暗号化されたコンテンツに対応する利用条件情報を生成する。

【０１６０】コンテンツ管理プログラム１１１は、圧縮され、暗号化されたコンテンツを利用条件情報とともに、コンテンツデータベース１１４に供給する。

【０１６１】コンテンツデータベース１１４は、コンテンツ管理プログラム１１１から受信したコンテンツに対応するコンテンツファイル１６１及び利用条件ファイル１６２を生成して、コンテンツファイル１６１にコンテンツを格納するとともに、利用条件ファイル１６２に利用条件情報を格納する。

【０１６２】コンテンツ管理プログラム１１１は、コンテンツデータベース１１４にコンテンツ及びコンテンツに対応する利用条件情報が格納されたとき、録音プログラム１１３から受信したＣＤの情報及び利用条件情報を表示操作指示プログラム１１２に供給する。

【０１６３】表示操作指示プログラム１１２は、録音の処理でコンテンツデータベース１１４に格納されたコンテンツに対応する利用条件情報及びＣＤの情報を基に、表示データファイル１８２に格納する表示用のデータを生成する。

【０１６４】録音プログラム１１３が表示させるウィンドウには、更に、ＣＤから読み出したコンテンツをコンテンツデータベース１１４に記録したとき、自動的に、ＣＤから読み出したコンテンツをポータブルデバイス６にチェックアウトさせるか否かの設定を行うボタン２５５が配置されている。

【０１６５】例えば、ボタン２５５がクリックされたとき、録音プログラム１１３は、ポータブルデバイス６を示すプルダウンメニューを表示する。使用者が、そのプルダウンメニューからポータブルデバイス６の選択をしたとき、選択されたポータブルデバイス６に自動的に、ＣＤから記録したコンテンツをチェックアウトする。使用者が、そのプルダウンメニューから”チェックアウトしない”を選択した場合、パーソナルコンピュータ１は、ＣＤからコンテンツを記録したとき、チェックアウトしない。

【０１６６】このように、録音プログラム１１３が表示させるウィンドウのボタン２５５をアクティブにしておくだけで、ＣＤから読み出したコンテンツがコンテンツデータベース１１４に記録されたとき、パーソナルコンピュータ１は、予め指定されているポータブルデバイス６に、ＣＤから読み出したコンテンツをチェックアウトさせることができる。

【０１６７】（２）異なるフォーマット間での取り扱い

ところで、音楽コンテンツを提供するコンテンツ配信業者は、数多く存在し、それぞれの配信業者毎に、そのコンテンツの暗号化方式や圧縮方式、さらに、利用条件情報のフォーマットが異なっている。従って、一般にユーザは、提供を受けたいコンテンツの配信業者毎に、再生やチェックイン／チェックアウト用のコンテンツ管理アプリケーションやポータブルデバイスを購入しなければならなかった。そのため、ユーザは、１つのパーソナルコンピュータ上に格納されている音楽コンテンツを、１つの管理アプリケーションやポータブルデバイスで取り扱うことができなかった。

【０１６８】そこで、本システムでは、このように配信業者毎にフォーマットが異なるコンテンツを、パーソナルコンピュータ１上で統一的に取り扱っている。

【０１６９】以下、この音楽コンテンツ配信システムにおける、配信業者毎にフォーマットが異なるコンテンツの統一的な取り扱いについて、図７を参照して説明する。

【０１７０】ネットワーク２に接続された複数のＥＭＤサーバは、例えば音楽提供会社Ａから提供される音楽コンテンツを配信するＥＭＤサーバ（Ａ）４－１、音楽提供会社Ｂから提供される音楽コンテンツを配信するＥＭＤサーバ（Ｂ）４－２、音楽提供会社Ｘから提供される音楽コンテンツを配信するＥＭＤサーバ（Ｘ）４－３であるものとする。各ＥＭＤサーバ４（４－１，４－２，４－３）は、各社独自にラインナップがされた音楽コンテンツを、ユーザが持つパーソナルコンピュータ１にネットワーク２を介して提供を行う。また、各ＥＭＤサーバ４（４－１，４－２，４－３）では、音楽コンテンツの暗号化方式、利用条件（Usage Rule）情報のフォーマット、音楽コンテンツの圧縮方式、音楽コンテンツの課金方式等が各社独自の方式が採用されそれぞれ異なる方式により音楽コンテンツを配信している。

【０１７１】パーソナルコンピュータ１には、音楽コンテンツの再生や管理等を行うためのアプリケーションソフトウェアとして、ＥＭＤサーバ（Ａ）４－１から音楽コンテンツの購入や管理や再生を行う再生用アプリケー

ション（Ａ）３１１と、ＥＭＤサーバ（Ｂ）４－２から音楽コンテンツの購入や管理や再生を行う再生用アプリケーション（Ｂ）３１２と、音楽コンテンツをポータブルデバイス（Ａ）６－１に転送するデバイスドライバ（Ａ）３１３と、音楽コンテンツをポータブルデバイス（Ｂ）６－２に転送するデバイスドライバ（Ｂ）３１４とがインストールされている。なお、この図７で示す再生用アプリケーション３１１，３１２は、図４で示した購入用アプリケーションプログラム１１５及びドライバ１１７に対応するものである。

【０１７２】また、パーソナルコンピュータ１には、ＨＤＤ２１内に格納されている全ての音楽コンテンツの包括的な管理を行う包括管理ユニット（Ｘ）３１５がインストールされている。この包括管理ユニット（Ｘ）３１５は、さらに、ＥＭＤ用受信インターフェース３１６，ＥＭＤ用送信インターフェース３１７，ＰＤ用ドライバ３１８により構成されている。

【０１７３】また、ここでは、ポータブルデバイス（Ａ）６－１は音楽提供会社Ａに対応した専用の装置であり、ポータブルデバイス（Ｂ）６－２は音楽提供会社Ｂに対応した専用の装置であり、ポータブルデバイス（Ｘ）６－３は音楽提供会社Ｘに対応した専用の装置であるものとする。なお、ここでは、メモリカード内に格納した音楽コンテンツは、各音楽提供会社独自の暗号化方式で暗号化されており、また、その圧縮方式や利用条件情報のフォーマットも異なる。そのため、例えば他のデバイスドライバ等と直接接続して、音楽コンテンツを転送することはできないようになっているものとする。

【０１７４】再生用アプリケーション（Ａ）３１１は、ＥＭＤサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ，コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この再生用アプリケーション（Ａ）３１１は、対応しているＥＭＤサーバに対してのみ接続処理を行うようになっている。ここでは、再生用アプリケーション（Ａ）３１１は、ＥＭＤサーバ（Ａ）４－１に対応した処理を行い、他のＥＭＤサーバに対して接続処理を行うことができない。また、再生用アプリケーション（Ａ）３１１は、ＥＭＤサーバ（Ａ）４－１と接続した際の認証処理、ポータブルデバイス（Ａ）６－１と接続した際の認証処理、ＨＤＤ２１に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。再生用アプリケーション（Ａ）３１１は、例えば、ＥＭＤサーバ（Ａ）４－１からダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、ＨＤＤ２１に格納する。なお、暗号化処理の方式は、各再生用アプリケーションでそれぞれ独自の方式を採用している。そのため、パーソナルコンピュータ１内の同一のＨＤＤ２１に格納されている音楽コンテンツであっても、専用の再生用アプリケーションでなければ、他の再生用アプリケーションでは暗号を解読することができないようになっている。

【０１７５】また、再生用アプリケーション（Ａ）３１１は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、再生用アプリケーション（Ａ）３１１は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を１回分デクリメントする等の処理を行う。

【０１７６】また、再生用アプリケーション（Ａ）３１１は、自己がＨＤＤ２１上に管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット（Ｘ）３１５のＥＭＤ用受信インターフェース３１６に送信する。

【０１７７】再生用アプリケーション（Ｂ）３１２は、ＥＭＤサーバとの接続処理、ログファイル等をアップロードする処理、音楽コンテンツ，コンテンツ鍵及び利用条件情報等をダウンロードする処理等を行う。この再生用アプリケーション（Ｂ）３１２は、対応しているＥＭＤサーバに対してのみ接続処理を行うようになっている。具体的には、再生用アプリケーション（Ｂ）３１２は、ＥＭＤサーバ（Ｂ）４－２に対応した処理を行い、他のＥＭＤサーバに対して接続処理を行うことができない。また、再生用アプリケーション（Ｂ）３１２は、ＥＭＤサーバ（Ｂ）４－２と接続した際の認証処理、ポータブルデバイス（Ｂ）６－２と接続した際の認証処理、ＨＤＤ２１に格納している音楽コンテンツ及び利用条件情報の暗号化／暗号解読処理等を行う。再生用アプリケーション（Ｂ）３１２は、例えば、ＥＭＤサーバ（Ｂ）４－２からダウンロードした音楽コンテンツ及びその利用条件情報をコンテンツ鍵で暗号化し、このコンテンツ鍵をセッション鍵で暗号化して、ＨＤＤ２１に格納する。

【０１７８】また、再生用アプリケーション（Ｂ）３１２は、各音楽コンテンツに付加されている利用条件情報の管理も行う。例えば、再生用アプリケーション（Ｂ）３１２は、利用条件情報に再生回数限度値が記述され、コンテンツの再生回数の制限がされている場合には、再生や複製を行う度に、再生や複製の回数限度値を１回分デクリメントする等の処理を行う。

【０１７９】また、再生用アプリケーション（Ｂ）３１２は、自己がＨＤＤ２１上に管理している音楽コンテンツ及び利用条件情報を、包括管理ユニット（Ｘ）３１５のＥＭＤ用受信インターフェース３１６に送信する。

【０１８０】デバイスドライバ（Ａ）３１３は、ポータブルデバイス（Ａ）６－１への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ（Ａ）３１３は、ポータブルデバイス（Ａ）６－１に音楽コンテンツを転送する。

【０１８１】デバイスドライバ（Ｂ）３１４は、ポータ

ブルデバイス（Ｂ）６－２への音楽コンテンツの転送等を行うアプリケーションソフトウェアである。デバイスドライバ（Ｂ）３１４は、ポータブルデバイス（Ｂ）６－２に音楽コンテンツを転送する。

【０１８２】包括管理ユニット（Ｘ）３１５は、ＥＭＤサーバ（Ｘ）４－３から音楽コンテンツの提供を受ける音楽提供会社Ｘ専用のアプリケーションソフトウェアであるとともに、デバイスドライバ（Ａ）３１３及びデバイスドライバ（Ｂ）３１４や、再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２との間で音楽コンテンツ及び利用条件情報の転送を行って、パーソナルコンピュータ１内の音楽コンテンツを包括的に管理を行う管理ソフトウェアでもある。また、自己が管理を行う音楽コンテンツを、携帯型の音楽再生装置である専用のポータブルデバイス（Ｘ）６－３に転送することができる。

【０１８３】なお、この包括管理ユニット（Ｘ）１１５は、図４に示したコンテンツ管理プログラム１１１に対応する処理を行う。

【０１８４】ＰＤ用ドライバ３１８は、ポータブルデバイス（Ｘ）６－３との接続用のインターフェースモジュールで、このポータブルデバイス（Ｘ）６－３との間における認証処理や暗号化処理を行う。また、ＰＤ用ドライバ３１８は、他のポータブルデバイス８，９に音楽コンテンツ等を転送する場合には、デバイスドライバ（Ａ）３１３やデバイスドライバ（Ｂ）３１４を介して音楽コンテンツ及び利用条件情報を転送する。

【０１８５】ＥＭＤ用受信インターフェース３１６は、再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２からの音楽コンテンツ及び利用条件情報の受信、ＥＭＤサーバ（Ｘ）４－３からネットワーク２を介して転送された音楽コンテンツ及び利用条件情報の受信、及び、ＰＤ用ドライバ３１８との間での音楽コンテンツ及び利用条件情報の送受信を行う。

【０１８６】ＥＭＤ用受信インターフェース３１６は、再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２から音楽コンテンツ及び利用条件情報を受信する場合には、相互認証処理、暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換等を行う。暗号化方式、利用条件情報、圧縮方式の変換は、再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２が用いている方式から、包括管理ユニット（Ｘ）３１５が用いている方式に変換される。ここで包括管理ユニット（Ｘ）３１５が用いている方式を、以下、統一転送プロトコルと呼ぶ。そして、ＥＭＤ用受信インターフェース３１６は、このように統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、ＰＤ用ドライバ３１８を介してデバイスドライバ（Ａ）３１３やデバイスドライバ（Ｂ）３１４に送信する。また、ＥＭＤ用受信インターフェース３１６は、統一転送プロトコルに変換した音楽コンテンツ及び利用条件情報を、ＰＤ用ドライバ３１８を介して、ポータブルデバイス（Ｘ）６－３に送信する。

【０１８７】このように、ＥＭＤサーバ（Ａ）４－１及びＥＭＤサーバ（Ｂ）４－２から提供される音楽コンテンツは、一旦再生用アプリケーション（Ａ）３１１及び再生用アプリケーション（Ｂ）３１２によりダウンロードされ、音楽コンテンツの暗号化方式、圧縮方式、利用条件情報が、統一転送プロトコルに変換されて、包括管理ユニット（Ｘ）３１５に転送される。包括管理ユニット（Ｘ）３１５は、ＥＭＤサーバ（Ａ）４－１、ＥＭＤサーバ（Ｂ４－２）、ＥＭＤサーバ（Ｘ）４－３からダウンロードされたそれぞれのコンテンツ提供会社の音楽コンテンツを統括的に管理を行うことができる。

【０１８８】また、ＥＭＤ用受信インターフェース３１６は、音楽コンテンツの複製（コピー）、移動（ムーブ）、チェックイン、チェックアウトの機能を有している。

【０１８９】ＥＭＤ用受信インターフェース３１６は、ユーザからの複製命令、移動命令に従い、例えば、再生用アプリケーション（Ａ）３１１や再生用アプリケーション（Ｂ）３１２によって管理されている音楽コンテンツを、包括管理ユニット（Ｘ）３１５に複製や移動する処理を行う。この際に、ＥＭＤ用受信インターフェース３１６は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットの変換を行って、統一転送プロトコルとする。

【０１９０】また、ユーザからのＣＤリッピング命令やチェックイン命令に従い、コンパクトディスク等の外部メディアやポータブルデバイス６（６－１，６－２，６－３）に格納されている音楽コンテンツを、包括管理ユニット（Ｘ）３１５に複製やチェックインする処理を行う。この際に、ＥＭＤ用受信インターフェース３１６は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。

【０１９１】また、ユーザからのチェックアウト命令に従い、包括管理ユニット（Ｘ）３１５により管理されている音楽コンテンツを、ポータブルデバイス（Ｘ）６－３に記録する処理を行う。この際に、ＥＭＤ用受信インターフェース３１６は、音楽コンテンツの暗号化方式及び圧縮方式、利用条件の記述フォーマットが統一転送プロトコルとされていなければ、これらの変換を行って、統一転送プロトコルとする。また、この際に、利用条件のチェックアウト可能回数を１減少させる。

【０１９２】また、包括管理ユニット（Ｘ）３１５では、図８に示すように、アプリケーション層の下位レイ

ヤに統一転送プロトコルを設けて、このレイヤにおいて他の再生用アプリケーションとのデータ転送を行っている。そして、包括管理ユニット（Ｘ）３１５は、この統一転送プロトコルの更に下位レイヤをｈｔｔｐ（ hiper Text Transfer Protocol ）として、ＥＭＤサーバ（Ｘ）４－３とのデータ送受信を行っている。

【０１９３】以上のような構成の音楽コンテンツ配信システムでは、ＥＭＤサーバ（Ａ）４－１及びＥＭＤサーバ（Ｂ）４－２から配信された音楽コンテンツを、包括管理ユニット（Ｘ）３１５が取得し、再生や管理を行うようになっている。そして、ＥＭＤサーバ（Ｘ）４－３、ＥＭＤサーバ（Ａ）４－１及びＥＭＤサーバ（Ｂ）４－２から配信された音楽コンテンツを、ポータブルデバイス（Ｘ）６－３へ転送できるようになっている。

【０１９４】このように音楽コンテンツ配信システムでは、包括管理ユニット（Ｘ）３１５を中心として、各再生用アプリケーション及びデバイスドライバの間で、転送する音楽コンテンツの暗号化方式の変換、転送する音楽コンテンツに付加された利用条件情報のフォーマットの変換、転送する音楽コンテンツの圧縮方式の変換が行われ、統一転送プロトコルを用いて音楽コンテンツの転送が行われる。そのため、例えば、再生用アプリケーション（Ａ）３１１によりＥＭＤサーバ（Ａ）４－１からダウンロードした音楽コンテンツ並びに再生用アプリケーション（Ｂ）３１２によりＥＭＤサーバＢ４－２からダウンロードした音楽コンテンツを、包括管理ユニット（Ｘ）３１５に転送することができる。このため、例えば音楽提供会社Ａからのみ提供されるアーチストの音楽コンテンツを、ポータブルデバイス（Ｘ）６－３に転送することができる。すなわち、この音楽コンテンツ配信システムでは、音楽コンテンツの暗号化方式、利用条件情報のフォーマット、音楽コンテンツの圧縮方式等を、統一転送プロトコルに変換するので、パーソナルコンピュータ１のハードディスク内に格納されている様々な方式の音楽コンテンツを、包括管理ユニット（Ｘ）３１５やポータブルデバイス（Ｘ）６－３により再生を行うことができる。特に、音楽コンテンツ配信システムでは、転送の際に、暗号化方式及び利用条件情報を変換するので、音楽コンテンツの著作権の保護を図りつつ、その音楽コンテンツの取り扱いの自由度を大きくすることができる。

【０１９５】すなわち、音楽コンテンツ配信システムでは、音楽コンテンツの再生や制御を行う再生用アプリケーション間で、少なくとも暗号化方式と利用条件情報の変換を行って、音楽コンテンツ及び利用条件情報の転送を行う。このことにより、音楽コンテンツ配信システムでは、複数の再生用アプリケーションが存在してもパーソナルコンピュータ１内の例えばＨＤＤ２１に格納されている音楽コンテンツを自由に移動させることができ、統一的な音楽コンテンツの管理をすることができる。また、音楽コンテンツとともに利用条件情報も転送するので、１つの音楽コンテンツに対して利用条件が重複したりすることがなく、音楽コンテンツの著作権も確実に保護することができる。

【０１９６】（３）利用条件情報

（一般的に用いられる利用条件情報の説明）つぎに、再生用アプリケーション（Ａ）３１１に用いられる利用条件情報のフォーマットの一例について説明をする。

【０１９７】再生用アプリケーション（Ａ）３１１では、例えば、図９（ａ）に示すような表形式で記述された利用条件情報が用いられている。

【０１９８】表の左欄には、利用条件のポリシーが列方向に記述され、右欄には各ポリシーの具体的な値が記述される。例えば、ポリシーとして、再生開始可能日（ｆｒｏｍ）、再生終了日（ｔｏ）、１回の再生に対する価格（ｐａｙ／ｐｌａｙ）等が記述される。このような利用条件情報は、図９（ｂ）に示すように各音楽コンテンツに付加された状態で、ＥＭＤサーバ（Ａ）４－１から配信される。再生用アプリケーション（Ａ）３１１は、記述されているポリシー及びその値に従い、音楽コンテンツの制御を行う。例えば、利用条件情報に、再生開始可能日（ｆｒｏｍ）が９９年１０月２５日、再生終了日（ｔｏ）が９９年１１月２４日、１回の再生に対する価格（ｐａｙ／ｐｌａｙ）がｙｅｓ／１０円と記述されているとする。この場合、その音楽コンテンツは、９９年１０月２５日から再生が可能とされ、それ以前にユーザから再生命令があっても、再生を禁止する。また、その音楽コンテンツは、９９年１１月２４日まで再生が可能とされ、それ以後となると、その音楽コンテンツを消去する。また、その音楽コンテンツは、１回の再生の度に１０円の課金を行うように設定されており、例えば、ユーザが再生した回数を別途ログ情報として保管しておき、そのログ情報をＥＭＤサーバ（Ａ）４－１にアップロードして、視聴したユーザに対して視聴した回数分だけの課金処理を行う。

【０１９９】（包括管理ユニット（Ｘ）３１５が用いている利用条件情報の説明）つぎに、包括管理ユニット（Ｘ）３１５が用いている利用条件情報について説明する。以下説明をする利用条件情報は、ＥＭＤサーバ（Ｘ）４－３からダウンロードされる音楽コンテンツに付加されており、上記包括管理ユニット（Ｘ）３１５がその音楽コンテンツの制御を行う際に用いられる。また、この利用条件情報は、再生用アプリケーション（Ａ）３１１と包括管理ユニット（Ｘ）３１５との間、及び、再生用アプリケーション（Ｂ）３１２と包括管理ユニット（Ｘ）３１５との間で、音楽コンテンツの転送をする際の統一フォーマットとして用いられる。以下、この利用条件情報を、統一利用条件情報と称する。

【０２００】統一利用条件情報は、図１０に示すように、インデックスファイル３３１、オートマトンファイ

ル３３２と、パラメータファイル３３３と、履歴ファイル３３４とから構成される。各ファイルは、ＸＭＬ（eXtensible Markup Language）言語で記述されている。

【０２０１】インデックスファイル３３１には、各ファイルのリファレンス情報等が記述されている。

【０２０２】オートマトンファイル３３２には、図１１に示すように、利用条件がオートマトンで記述されたオートマトン記述部３４１と、コンテンツ鍵による認証コード（ＭＡＣ:Message Authentication Code）３４２、コンテンツ提供者の署名（Ｓｉｇ）３４３、この署名を検証するための認証書（Ｃｅｒｔ）３４４が付加されている。ここで、コンテンツ鍵をK_C、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれK^{-1}_E，K^{1}_Eとする。

【０２０３】オートマトン記述部３４１は、tuple列で記述されたExtended State Machineにより音楽コンテンツの動作状態が記述される。

【０２０４】具体的には、オートマトン記述部３４１では、現在の音楽コンテンツの動作状態の集合をＱとし、音楽コンテンツのイベントを表す入力シンボルの集合をΣとし、状態遷移した後の音楽コンテンツの動作状態の集合をＱ′を以下のように表す。

Ｑ′＝｛ｄ｜ｄ＝δ（ｑ，α）｜ｑ　Ｑ，α　Σ，δ：Ｑ×Σ→Ｑ｝

この式に示すように、状態遷移した後の状態Ｑ′の集合は、ｄとして表される。このｄは、変数ｑ、αをもった関数δによって定義される。ｑは、音楽コンテンツの動作状態の集合Ｑのなかの１つの動作状態を示している。αは、イベントの集合Σのなかの１つのイベントを示している。そして、関数δは、Ｑ及びΣのべき集合のＱへの写像である。

【０２０５】そして、以上のＱ，Σ，Ｑ′に基づき、各tupleを

｛〈ｑ，α，ｄ〉｜ｑ，ｄ　Ｑ，α　Σ｝

として表す。なお、〈ｑ，α，ｄ〉は、ｑ、α、ｄの順列のある組み合わせを示している。

【０２０６】ここで、Σには、再生（Play），複製（copy），支払い金額（pay Y），再生開始可能日時（from YMD），再生終了日時（to YMD），使用可能日数（in Ddays），ヌルイベント（ε）といったイベントが、以下のように記述される。

Σ＝｛Play,copy,pay Y,from YMD,to YMD,in Ddays,ε｝

このようにオートマトン記述部３４１は、以上のように記述される。

【０２０７】このオートマトン記述部３４１への具体的な記述例について説明をする。

【０２０８】例えば、図１２に示すような音楽コンテンツの動作遷移を示すオートマトンのtuple列による記述例を、図１３に示す。

【０２０９】このオートマトンは、以下に説明するような状態遷移をする。

【０２１０】まず、初期状態ｑ０から、状態ｑ１及び状態ｑ５に遷移する。状態ｑ１及び状態ｑ５以降は、それぞれ並行して動作する。

【０２１１】状態ｑ１で、所定金額（例えば１０円）の支払いイベント（ｐａｙ１０）が発生すると状態ｑ２へ遷移する。状態ｑ２で、プレイイベント（ｐｌａｙ）が発生すると状態ｑ１へ遷移する。すなわち、このオートマトンでは、１０円の支払いがされると、音楽コンテンツが１回だけ再生が可能となることを示している。また、状態ｑ１で、所定金額（例えば１０００円）の支払いイベント（ａ．ｐａｙ１０００）が発生すると状態ｑ３へ遷移する。状態ｑ３では、プレイイベント（ｐｌａｙ）が発生すると、再度この状態ｑ３に遷移する。すなわち、このオートマトンでは、１０００円の支払いがされると、音楽コンテンツが回数に制限無く再生が可能となることを示している。また、状態ｑ１で、一回の再生金額（例えば１０円）のｎ倍の金額の支払いイベント（ｐａｙ１０×ｎ）が発生すると、状態ｑ４へ遷移する。状態ｑ４へ遷移してから、プレイイベント（ｐｌａｙ）が発生すると、再度この状態ｑ４に遷移する。そして、この状態ｑ４で、ｎ回のプレイイベントが発生すると、状態ｑ１に遷移する。すなわち、このオートマトンでは、１０×ｎ円の支払いがされると、音楽コンテンツがｎ回再生が可能となることを示している。

【０２１２】また、状態ｑ５で、所定金額（例えば１００円）の支払いイベント（ｐａｙ１００）が発生すると状態ｑ６へ遷移する。状態ｑ６で、コピーイベント（ｃｏｐｙ）が発生すると状態ｑ５へ遷移する。また、状態ｑ６で、コピーイベント（ｃｏｐｙ）が発生すると、状態ｑ８へ遷移する。状態ｑ８で、プレイイベント（ｐｌａｙ）が発生すると、再度この状態ｑ８に遷移する。また、この状態ｑ８で、コピーイベント（ｃｏｐｙ）が発生すると、状態ｑ９に遷移する。状態ｑ９では、どの状態へも遷移せずイベントも発生できない終端状態である。すなわち、このオートマトンでは、１００円の支払いがされると音楽コンテンツを他のデバイスへ１回コピーすることができることを示している。また、このオートマトンでは、コピーされた音楽コンテンツを再生することは何回でも可能であるが、他のデバイス等にコピーした場合には、再生ができなくなることを示している。

【０２１３】また、状態ｑ５で、所定金額（例えば２０００円）の支払いイベント（ａ．ｐａｙ２０００）が発生すると状態ｑ７へ遷移する。状態ｑ７では、コピーイベント（ｃｏｐｙ）が発生すると、再度この状態ｑ７に遷移する。また、状態ｑ７で、コピーイベント（ｃｏｐｙ）が発生すると、状態ｑ８へ遷移する。状態ｑ８で、プレイイベント（ｐｌａｙ）が発生すると、再度この状態ｑ８に遷移する。また、この状態ｑ８で、コピーイベ

ント（ｃｏｐｙ）が発生すると、状態ｑ９に遷移する。状態ｑ９では、どの状態へも遷移せずイベントも発生できない終端状態である。すなわち、このオートマトンでは、２０００円の支払いがされると、音楽コンテンツを他のデバイスへ回数制限無くコピーすることができることを示している。また、このオートマトンでは、コピーされた音楽コンテンツを再生することは何回でも可能であるが、他のデバイス等にコピーした場合には、再生ができなくなることを示している。

【０２１４】そして、以上のように状態遷移をするオートマトンをtuple列で記述すると、図１３に示すようになる。

【０２１５】また、オートマトン記述部３４１は、音楽コンテンツの動作を更新するため、動作状態の並列合成を記述しても良い。例えば、動作a_0と動作a_1との並列合成は、tuple列で以下のように表される。

$\langle q_0,\ pay100,\ q_1,\ a.n:=a.n-100\rangle$　・・・（1）

$\langle q_0,\ pay(a.n),\ q_1,\ a.n:=0\rangle$　・・・（2）

$\langle q_1,\ play,\ q_2\rangle$　・・・（3）

この例は、１つの音楽コンテンツの買い取り値段｛式（１）｝が、アルバム買い取り｛式（２）｝の値段に影響を及ぼすことを示している。

【０２１６】以上のようなオートマトン記述部３４１は、図１４に示すように、エントリーＩＤ３４５と、コンテンツＩＤ３４６と、バージョン情報３４７と、変数情報３４８と、tuple列３４９とから構成される。

【０２１７】以上のように記述フォーマットが定められたオートマトン記述部３４１の具体例について説明をする。

【０２１８】なお、以下にオートマトンの記述で用いられているイベント及びコマンドは、ＸＭＬの仕様に基づいて規定されたＤＴＤ（ Document Type Definition ）で定義されている。例えば、図１５に示すように、再生動作（play）、複製動作（copy）、再生権購入（pay-for-play）、複製権購入（pay-for-copy）、アルバム再生権購入（pay-for-album-play）、アルバム複製権購入（pay-for-album-copy）、使用可能開始日（from）、使用終了日（to）、ヌル動作（null）がイベントとして、ＤＴＤによって定義されている。

【０２１９】図１６は、音楽コンテンツが１９９９年９月１日から再生が可能であることを示すＸＭＬ言語によるオートマトン記述部３４１の記述例である。

【０２２０】この図１６に示す記述は、図１７に示すようなオートマトンとなる。このオートマトンは、初期状態の状態ｑ１と、状態ｑ２とから構成される。状態ｑ１で、日付が使用可能開始日（ｆｒｏｍ）の１９９９年９月１日となると、状態ｑ２へ遷移する。そして、状態ｑ２で、再生イベント（ｐｌａｙ）が発生すると、音楽コンテンツの再生を行い、再度状態ｑ２へ遷移する。このようにこのオートマトンは、音楽コンテンツを、１９９９年９月１日から再生を可能とするように制御している。

合成は、tuple列で以下のように表される。

$\langle q_0,\ \alpha,\ a_0,\ q_0\rangle$

$\langle q_0,\ \alpha,\ a_1,\ q_0\rangle$

また、オートマトン記述部３４１には、状態遷移に伴うアクションを記述してもよい。例えば、アクションは、tupleで以下のように表される。

$\langle q_0,\ \alpha,\ q_1;action\rangle$

このアクションは、予め定義した変数を用いた関数として表される。また、変数は、ＩＤとスコープと初期値とからなる。スコープには、その音楽コンテンツ、アルバム、システム全体等のクラスがある。例えば、アルバム（ａ）の買い取りの値段を表す変数をｎとし、ａ．ｎ：＝１０００のように記述する。このように変数に対するアクションが記述されたオートマトン記述部３４１の一例を以下に示す。

```
<q0, pay100, q1, a.n:=a.n-100> ・・・（1）
<q0, pay(a.n), q1, a.n:=0>     ・・・（2）
<q1, play, q2>                 ・・・（3）
```

る。

【０２２１】図１８は、音楽コンテンツが１９９９年１０月３１日まで再生が可能であることを示すＸＭＬ言語によるオートマトン記述部３４１の記述例である。

【０２２２】この図１８に示す記述は、図１９に示すようなオートマトンとなる。このオートマトンは、初期状態の状態ｑ１と、終端状態の状態ｅｎｄとから構成される。状態２で、再生イベント（ｐｌａｙ）が発生すると、音楽コンテンツの再生を行い、再度状態ｑ２へ遷移する。また、状態２で、使用終了日（ｔｏ）の１９９９年１０月３１日となると、状態ｅｎｄへ遷移する。状態ｅｎｄとなると、どの状態へも遷移せずイベントも発生しない。このように、このオートマトンは、音楽コンテンツを、１９９９年１０月３１日まで再生を可能とするように制御している。

【０２２３】図２０は、音楽コンテンツの再生可能期間が１９９９年９月１日から１９９９年１０月３１日までであって、且つ、その再生可能回数が１６回であることを示すＸＭＬ言語によるオートマトン記述部３４１の記述例である。

【０２２４】この図２０に示す記述は、図２１に示すようなオートマトンとなる。このオートマトンは、初期状態の状態ｑ１と、状態ｑ２と、終端状態の状態ｅｎｄとから構成される。状態ｑ１で、使用可能開始日（ｆｒｏｍ）の１９９９年９月１日となると、状態ｑ２へ遷移する。そして、状態ｑ２で、再生イベント（ｐｌａｙ）が発生すると、音楽コンテンツの再生を行い、再度状態ｑ２へ遷移する。また、状態２で、使用終了日（ｔｏ）の１９９９年１０月３１日となるか、或いは、１６回再生イベント（ｐｌａｙ×１６）が発生すると、状態ｅｎｄへ遷移する。状態ｅｎｄとなると、どの状態へも遷移せずイベントも発生しない。このようにこのオートマトン

は、音楽コンテンツの再生期間を１９９９年９月１日から１９９９年１０月３１日までとし、且つ、その再生回数を１６回に制御している。

【０２２５】図２２は、音楽コンテンツの再生回数を１６回に制限することを示すＸＭＬ言語によるオートマトン記述部３４１の記述例である。

【０２２６】つぎに、パラメータファイル３３３には、図２３に示すように、パラメータ記述部３５１、コンテンツ鍵による認証コード３５２、コンテンツ提供者の署名３５３、この署名を検証するための認証書３５４が付加されている。ここで、コンテンツ鍵をK_C、コンテンツを作成したコンテンツ提供者のプライベート鍵及びパブリック鍵をそれぞれK^{-1}_E，K^1_Eとする。

【０２２７】また、パラメータファイル３３３は、上記オートマトンファイル３３２を作成したコンテンツ提供者とは別のコンテンツ提供者（例えば、コンテンツ小売業者やコンテンツ中間業者等の二次提供者）により書き換えることが可能である。書き換えられたパラメータファイル３３３は、図２４に示すように、それぞれの提供者や中間業者等に与えられたユニークなエンティティＩＤ５５が付加される。ここで、K'_Cは、二次提供者のコンテンツ鍵で、$K'_C=H(K_C, EntityID)$となる。なお、ここで、Hは、一方向ハッシュ関数である。二次提供者のコンテンツ鍵K'_Cは、一次提供者のコンテンツ鍵K_Cから作成される。一次提供者と二次提供者とは、その認証書により区別される。

【０２２８】パラメータファイル３３３を検証する方法としては、コンテンツ鍵が得られていればＭＡＣにより行い、安全性等の理由でコンテンツ鍵が得られない場合には署名と証明書により検証する。

【０２２９】ＭＡＣにより検証するプロトコルは以下のようになる。コンテンツの一次提供者をＳ、二次提供者をＡ、端末をＢとする。Ｓ→Ａは、ＳからＡへの伝送を示しており、Ｓ→Ｂは、ＳからＢへの伝送を示しており、Ａ→Ｂは、ＡからＢへの伝送を示している。また、ID_Aは、デバイスＡのＩＤを示している。

【０２３０】Ｓ→Ａ：　$K'_C=H(K_C, ID_A)$

Ｓ→Ｂ：　$X=E_{Ks}(K_C)$

Ａ→Ｂ：　ID_A, Parameters, $M=MAC_{K'_C}$(Parameters)

Ｂ：　$M \stackrel{?}{=} MAC_{K'_C}$(Parameters)

このパラメータ記述部３５１には、上記オートマトンファイル３１のオートマトン部４１に記述された値の変更のための関数の係数が記述される。例えば、図１３に示した例において、オートマトン部４１では、例えば、以下のように音楽コンテンツの価格が関数となる場合がある。

$\langle q_0, pay(f_1(10)), q_1\rangle$

$\langle q_1, pay(f_2(10)\times n), q_2\rangle$

この場合、上記関数f_1及びf_2を、例えば、以下のように定める。

$f_1(n)=0.9n$

$f_2(n)=90+0.1n$

このように関数を定めることによって、例えば、一次提供者が価格のデフォルト値を定め、二次提供者がパラメータファイル３３３を書き換えて、価格を変更することができる。

【０２３１】以上のようなパラメータ記述部３５１は、図２５に示すように、エントリーＩＤ３５６と、コンテンツＩＤ３５７と、係数情報３５８とから構成される。

【０２３２】履歴ファイル３３４は、オートマトン記述部３４１に記述内容に基づき動作する音楽コンテンツの動作の軌跡を記述するファイルである。この履歴ファイル３３４には、上記オートマトン記述４１のｔｕｐｌｅ内のステータスと変数を記録する。例えば、上述した図１３に例において、２回再生を行った場合には、

$\langle q_0, q_1, q_0, q_1\rangle$

となり、これにより以下のような動作の軌跡を得ることができる。

〈ｐａｙ１０，ｐｌａｙ，ｐａｙ１０，ｐｌａｙ〉

これを集計して、例えば、包括管理ユニット（Ｘ）３１５にアップロード等すれば、ユーザの支払い金額を計算することができる。

【０２３３】以上のように音楽コンテンツ配信システムでは、ポリシー自体及びその具体的な値をプログラム化したオートマトンによって利用条件情報を記述しているので、コンテンツの利用条件の記載の自由度を高めることができる。

【０２３４】（４）破壊された音楽コンテンツ等のリストア及び再ダウンロード

つぎに、包括管理ユニット（Ｘ）３１５による音楽コンテンツのバックアップについて説明をする。

【０２３５】まず、包括管理ユニット（Ｘ）３１５の音楽コンテンツの鍵管理方法について、図２６を用いて説明する。

【０２３６】包括管理ユニット（Ｘ）３１５は、パーソナルコンピュータ１内のＨＤＤ２１に、音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎを格納している。また、包括管理ユニット（Ｘ）３１５は、各音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎに対応するコンテンツ鍵Ｋｃ１，Ｋｃ２，Ｋｃ３・・・Ｋｃｎも格納している。コンテンツ鍵Ｋｃは、音楽コンテンツＣに対して一対一の関係となっている。また、各音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎには、それぞれの識別するためのコンテンツＩＤが付加されている。このコンテンツＩＤを、ＣＩＤ１，ＣＩＤ２，ＣＩＤ３・・・ＣＩＤｎとする。

【０２３７】音楽コンテンツＣ１，Ｃ２，Ｃ３・・・Ｃｎは、コンテンツ鍵Ｋｃ１，Ｋｃ２，Ｋｃ３・・・Ｋｃｎにより暗号化され、Ｅ（Ｋｃ１，Ｃ１），Ｅ（Ｋｃ２，Ｃ２），Ｅ（Ｋｃ３，Ｃ３）・・・Ｅ（Ｋｃｎ，Ｃ

ｎ）とされた状態でパーソナルコンピュータ１のＨＤＤ２１内に記録されている。ここで、Ｅ（Ｋ，Ｃ）は、鍵Ｋでコンテンツ Ｃを暗号化していることを示す。通常、コンテンツＩＤは、音楽コンテンツＣのヘッダなどに記録されて音楽コンテンツＣとともに暗号化されているか、或いは、ＭＡＣが音楽コンテンツＣに付加された状態とされており、音楽コンテンツ本体と切り離しができないようになっている。

【０２３８】また、コンテンツ鍵Ｋｃ１，Ｋｃ２，Ｋｃ３・・・Ｋｃｎは、ストレージ鍵ＫＳにより暗号化され、Ｅ（ＫＳ，Ｋｃ１），Ｅ（ＫＳ，Ｋｃ２），Ｅ（ＫＳ，Ｋｃ３）・・・Ｅ（ＫＳ，Ｋｃｎ）とされた状態でパーソナルコンピュータ１のＨＤＤ２１上に記録されている。このストレージ鍵ＫＳは、いわゆる耐タンパ性を有しており、通常のユーザからは参照することができない記録領域に保存されている。

【０２３９】以上のように鍵管理が行われる包括管理ユニット（Ｘ）３１５では、例えば、音楽コンテンツＣ１の再生を行う場合には、ストレージ鍵ＫＳを用いてコンテンツ鍵Ｋｃ１の暗号を解除し、続いて、このコンテンツ鍵Ｋｃ１を用いて、音楽コンテンツＣ１の暗号を解除する。このことにより、包括管理ユニット（Ｘ）３１５は、音楽コンテンツＣ１の再生を行うことができる。

【０２４０】また、以上のように鍵管理が行われる包括管理ユニット（Ｘ）３１５では、例えば、音楽コンテンツＣ１をＨＤＤ２１からポータブルデバイス（Ｘ）６－３に移動（ＭＯＶＥ）する場合には、ポータブルデバイス（Ｘ）６－３との間で相互認証を行い、認証が完了するとストレージ鍵ＫＳを用いてコンテンツ鍵Ｋｃ１の暗号を解除し、続いて、セッション鍵によりコンテンツ鍵Ｋｃ１を暗号化し、暗号化したコンテンツ鍵Ｋｃ１及び暗号化した音楽コンテンツＣ１をポータブルデバイス（Ｘ）６－３に転送する。そして、コンテンツ鍵Ｋｃ１と音楽コンテンツＣ１をともにＨＤＤ２１から消去をする。このことにより、包括管理ユニット（Ｘ）３１５は、音楽コンテンツＣ１をポータブルデバイス（Ｘ）６－３に移動することができる。

【０２４１】つぎに、ＨＤＤ２１が破壊した場合など、音楽コンテンツやコンテンツ鍵をＨＤＤ２１から再生することができなくなったときにおける音楽コンテンツの復元方法について説明する。

【０２４２】まず、通常時において、包括管理ユニット（Ｘ）３１５は、暗号化した音楽コンテンツＣ及びコンテンツ鍵Ｋｃのバックアップデータを、ＨＤＤ２１内や他の記録媒体等に保存しておく。

【０２４３】また、通常時において、包括管理ユニット（Ｘ）３１５は、ＥＭＤサーバ（Ｘ）４－３からダウンロードした音楽コンテンツの購入記録と、ＨＤＤ２１内に記憶している全ての音楽コンテンツのコンテンツＩＤのリストとを、使用ログ情報として管理する。このログ情報は、音楽コンテンツをＥＭＤサーバ（Ｘ）４－３からダウンロードしたときや、ポータブルデバイス（Ｘ）６－３への移動等の音楽コンテンツの制御を行ったときに、更新するようにする。また、ログ情報は、ＨＤＤ２１の別領域や他の記録媒体に格納しておく。包括管理ユニット（Ｘ）３１５は、このログ情報を、定期的、或いは、アクセスした度に、ＥＭＤサーバ（Ｘ）４－３にアップロードする。

【０２４４】そして、包括管理ユニット（Ｘ）３１５のＨＤＤ２１に格納されている音楽コンテンツＣやコンテンツ鍵Ｋｃが破壊されてしまった場合には、以下に示すような処理が行われる。

【０２４５】音楽コンテンツＣやコンテンツ鍵Ｋｃが破壊されてしまった場合、包括管理ユニット（Ｘ）３１５は、まず、ＥＭＤサーバ（Ｘ）４－３にアクセスを行って、ユーザ認証を行う。

【０２４６】続いて、ＥＭＤサーバ（Ｘ）４－３は、認証したユーザのユーザＩＤから、包括管理ユニット（Ｘ）３１５の使用ログ情報を参照して、整合検証値ＩＣＶ（Integrity Check Value）を生成する。この整合検証値ＩＣＶは、使用ログ情報に記述されている音楽コンテンツＣのコンテンツＩＤであるＣＩＤと、包括管理ユニット（Ｘ）３１５のストレージ鍵ＫＳとに基づき、以下のように生成される。ＩＣＶ＝Ｈ（ＫＳ，ＣＩＤ１｜｜ＣＩＤ２｜｜・・・｜｜ＣＩＤｎ）ここで、Ｈ（Ｋ，Ｄａｔａ）は、一方向ハッシュ関数で、鍵Ｋによりその値が変化するものである。

【０２４７】続いて、ＥＭＤサーバ（Ｘ）４－３は、生成した整合検証値ＩＣＶを、包括管理ユニット（Ｘ）３１５に送信する。

【０２４８】続いて、包括管理ユニット（Ｘ）３１５は、音楽コンテンツＣ又はコンテンツ鍵Ｋｃがバックアップされていれば、そのバックアップデータをリストアして、音楽コンテンツＣ又はコンテンツ鍵ＫｃをＨＤＤ２１内に保存する。また、音楽コンテンツＣ又はコンテンツ鍵Ｋｃがバックアップされていなければ、ＥＭＤサーバ（Ｘ）４－３から破壊された音楽コンテンツＣ又はコンテンツ鍵Ｋｃを再配信してもらう。このとき、ＥＭＤサーバ（Ｘ）４－３は、ユーザの購入履歴を参照して、以前に購入しているコンテンツであれば、課金処理を行わない。

【０２４９】包括管理ユニット（Ｘ）３１５は、以上の処理を行い、破壊された音楽コンテンツＣ又はコンテンツ鍵Ｋｃを復活させる。

【０２５０】そして、包括管理ユニット（Ｘ）３１５は、復活された音楽コンテンツＣ又はコンテンツ鍵Ｋｃの再生や制御を行う場合には、上記整合検証値ＩＣＶによりその音楽コンテンツのＣＩＤをチェックするようにする。このように、整合検証値ＩＣＶを用いて復活させた音楽コンテンツＣ又はコンテンツ鍵Ｋｃをチェックす

ることにより、例えば、ある音楽コンテンツＣｉをポータブルデバイス（Ｘ）６－３に移動してＨＤＤ２１上からは消去されている場合に、悪意のあるユーザが暗号化された音楽コンテンツＣｉであるＥ（Ｋｃｉ，Ｃｉ）を覚えておきリストアしたとしても、それらのデータは再生をすることもまた移動等の制御をすることもできない。

【０２５１】なお、音楽コンテンツＣ及びコンテンツ鍵Ｋｃではなく、ストレージ鍵ＫＳが破壊されている場合には、包括管理ユニット（Ｘ）３１５の再インストールを行う。この場合であっても、ＥＭＤサーバ（Ｘ）４－３にユーザ登録をするとともにログ情報をアップロードしておけば、上述した方法でリストアや再ダウンロードをすることができる。

【０２５２】このように、音楽コンテンツ配信システムでは、例えば、ハードディスクのクラッシュ等により、音楽コンテンツが破壊されてしまった場合であっても、著作権を保護しながら、復元することができる。例えば、その音楽コンテンツが正規に購入したものであれば、無料で復活させることができる。

【０２５３】（５）包括管理ユニットのマスター鍵及び認証鍵等の配布方法

包括管理ユニット（Ｘ）３１５とポータブルデバイス（Ｘ）６－３との間では、ポータブルデバイス（Ｘ）６－３の固有のＩＤ及び認証鍵（ＭＧ－ＩＤ／ＩＫ）と、包括管理ユニット（Ｘ）３１５の固有のマスター鍵（ＯＭＧ－ＭＫ）とを用いて、相互認証が行われる。

【０２５４】包括管理ユニット（Ｘ）３１５とポータブルデバイス（Ｘ）６－３との間で、相互認証が行われると、包括管理ユニット（Ｘ）３１５からポータブルデバイス（Ｘ）６－３へ音楽コンテンツを送信（チェックアウト）したり、ポータブルデバイス（Ｘ）６－３から包括管理ユニット（Ｘ）３１５への音楽コンテンツの返却（チェックイン）をしたりできるようになる。なお、包括管理ユニット（Ｘ）３１５は、パーソナルコンピュータ１のＨＤＤ２１内に暗号化した音楽コンテンツを保存しており、また、ポータブルデバイス（Ｘ）６－３は、内部のメモリカード等の記憶媒体に暗号化した音楽コンテンツを保存する。そのため、包括管理ユニット（Ｘ）３１５からポータブルデバイス（Ｘ）６－３へ音楽コンテンツを送信する場合には、パーソナルコンピュータ１のＨＤＤ２１上の音楽コンテンツが、ポータブルデバイス（Ｘ）６－３に装着されたメモリカード上に転送されることとなる。また、ポータブルデバイス（Ｘ）６－３から包括管理ユニット（Ｘ）３１５へ音楽コンテンツを送信する場合には、ポータブルデバイス（Ｘ）６－３に装着されたメモリカード上の音楽コンテンツが、パーソナルコンピュータ１のＨＤＤ２１上に転送されることとなる。

【０２５５】ポータブルデバイス（Ｘ）６－３は、ＩＤ情報（ＭＧ－ＩＤ）、複数世代分の認証鍵（ＭＧ－ＩＫ）及び複数世代分のマスター鍵（ＯＭＧ－ＭＫ）を工場出荷時から予め保持している。ポータブルデバイス（Ｘ）６－３には、後に外部からこれらの鍵等は供給されない。ポータブルデバイス（Ｘ）６－３は、必要に応じて、認証鍵（ＭＧ－ＩＫ）及びマスター鍵（ＯＭＧ－ＭＫ）の世代を更新する。ポータブルデバイス（Ｘ）６－３は、世代更新された最も新しい世代の認証鍵及びマスター鍵で相互認証を行い、旧世代の認証鍵及びマスター鍵では、相互認証を行わない。以下、ポータブルデバイス（Ｘ）６－３は、第０世代から第９９世代の１００世代分の認証鍵（ＭＧ－ＩＫ［０－９９］）及びマスター鍵（ＯＭＧ－ＭＫ［０－９９］）を保持しているものとする。なお、第ｉ世代の認証鍵を（ＭＧ－ＩＫ［ｉ］）と示し、第ｉ世代のマスター鍵を（ＯＭＧ－ＭＫ［ｉ］）と示す。

【０２５６】また、包括管理ユニット（Ｘ）３１５は、マスター鍵（ＯＭＧ－ＭＫ）を保持することによって、オーディオ用コンパクトディスク等からパーソナルコンピュータ１内に音楽コンテンツを転送して、保存することができる。また、包括管理ユニット（Ｘ）３１５は、マスター鍵（ＯＭＧ－ＭＫ）を保持することによって、ＥＭＤサーバ（Ｘ）４－３から音楽コンテンツをダウンロードして、パーソナルコンピュータ１内に保存することができる。

【０２５７】ここで、包括管理ユニット（Ｘ）３１５では、コンパクトディスクから音楽コンテンツを転送することはできるがＥＭＤサーバ（Ｘ）４－３からは音楽コンテンツをダウンロードすることができないマスター鍵（ＯＭＧ－ＭＫ）と、コンパクトディスクからもＥＭＤサーバ（Ｘ）４－３からも音楽コンテンツを転送することができるマスター鍵（ＯＭＧ－ＭＫ）とが異なったものとなっている。以下、コンパクトディスクから音楽コンテンツを転送することはできるがＥＭＤサーバ（Ｘ）４－３からは音楽コンテンツをダウンロードすることができない鍵のことを、リッピング専用鍵ともいい、コンパクトディスクからもＥＭＤサーバ（Ｘ）４－３からも音楽コンテンツを転送することができる鍵のことをＥＭＤ鍵ともいう。

【０２５８】なお、本例では、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）がリッピング専用鍵となっており、第１世代以後のマスター鍵（ＯＭＧ－ＭＫ［１～９９］）がＥＭＤ鍵となっている。

【０２５９】つぎに、リッピング専用鍵を用いた処理の手順について説明する。

【０２６０】包括管理ユニット（Ｘ）３１５がＣＤ－ＲＯＭからインストールされる場合には、図２７に示すように、包括管理ユニット（Ｘ）３１５のインストールソフトウェアが格納されたＣＤ－ＲＯＭ３６１とともに、ポータブルデバイス（Ｘ）６－３と、フロッピー（登録

商標）ディスク３６２とが例えばセットで販売される。フロッピーディスク３６２には、ポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ），第０世代の認証鍵（ＭＧ－ＩＫ［０］），第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）が格納されている。

【０２６１】続いて、販売されたポータブルデバイス（Ｘ）６－３等を使用可能とするには、まず、ＣＤ－ＲＯＭ３６１をパーソナルコンピュータ１に装着する（ステップＳ１１）。続いて、このＣＤ－ＲＯＭ３６１から包括管理ユニット（Ｘ）３１５をパーソナルコンピュータ１にインストールする（ステップＳ１２）。すると、包括管理ユニット（Ｘ）３１５がパーソナルコンピュータ１のハードディスク内に格納されることとなる（ステップＳ１３）。続いて、フロッピーディスク３６２に格納されているポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ）と、第０世代の認証鍵（ＭＧ－ＩＫ［０］）と、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）とをパーソナルコンピュータ１に保存する（ステップＳ１４）。

【０２６２】このことによって、包括管理ユニット（Ｘ）３１５は、音楽ＣＤ３６３等により提供される音楽コンテンツを、パーソナルコンピュータ１のハードディスク内に格納することができるようになる（ステップＳ１５）。なお、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）は、リッピング専用鍵なので、ＥＭＤサーバ（Ｘ）４－３から音楽コンテンツをダウンロードできないようになっている。

【０２６３】また、ポータブルデバイス（Ｘ）６－３は、世代更新がされていく１００世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第０世代とされている。このため、第０世代の認証鍵及びマスター鍵を保持している包括管理ユニット（Ｘ）３１５と、ポータブルデバイス（Ｘ）６－３との相互認証が可能となる。したがって、音楽ＣＤ３６３等により提供される音楽コンテンツを、ポータブルデバイス（Ｘ）６－３のメモリーカードに格納することができるようになる（ステップＳ１６）。

【０２６４】一方、包括管理ユニット（Ｘ）３１５がネットワークを介して提供される場合には、図２８に示すように、ポータブルデバイス（Ｘ）６－３とともに、インターネット上のＥＭＤ登録サーバ３のアドレス、ユーザＩＤ及びパスワード等が提供される。

【０２６５】続いて、販売されたポータブルデバイス（Ｘ）６－３等を使用可能とするには、まず、ユーザＩＤ及びパスワードを用いてネットワーク上のＥＭＤ登録サーバ３にアクセスをする（ステップＳ２１）。続いて、ＥＭＤ登録サーバ３は、ユーザＩＤ及びパスワードの認証を行う（ステップＳ２２）。続いて、認証に問題がなければ、ＥＭＤ登録サーバ３は、包括管理ユニット（Ｘ）３１５のインストールソフトウェアと、ポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ）と、第０世代の認証鍵（ＭＧ－ＩＫ［０］）と、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）とを、パーソナルコンピュータ１に送信する（ステップＳ２３）。続いて、パーソナルコンピュータ１は、包括管理ユニット（Ｘ）３１５のインストールソフトウェアを起動して、包括管理ユニット（Ｘ）３１５をインストールするとともに、ポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ）と、第０世代の認証鍵（ＭＧ－ＩＫ［０］）と、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）とをＨＤＤ２１に保存する（ステップＳ２４）。すると、ハードディスクには、包括管理ユニット（Ｘ）３１５が格納されることとなる（ステップＳ２５）。

【０２６６】このことによって、包括管理ユニット（Ｘ）３１５は、音楽ＣＤ３６３等により提供される音楽コンテンツを、パーソナルコンピュータ１のＨＤＤ２１内に格納することができるようになる（ステップＳ２６）。なお、第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）は、リッピング専用鍵なので、ＥＭＤサーバ（Ｘ）４－３から音楽コンテンツをダウンロードできないようになっている。

【０２６７】また、ポータブルデバイス（Ｘ）６－３は、世代更新がされていく１００世代分の認証鍵及びマスター鍵を内部に保持しているが、初期設定状態では、第０世代とされている。このため、第０世代の認証鍵及びマスター鍵を保持している包括管理ユニット（Ｘ）３１５と、ポータブルデバイス（Ｘ）６－３との相互認証が可能となる。したがって、音楽ＣＤ３６３等により提供される音楽コンテンツを、ポータブルデバイス（Ｘ）６－３のメモリカード内に格納することができるようになる（ステップＳ２７）。

【０２６８】なお、以上の図２７及び図２８に示した方法に限られず、包括管理ユニット（Ｘ）３１５及びリッピング専用の第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）をＣＤ－ＲＯＭ３６１に格納しておき、ポータブルデバイス（Ｘ）６－３との認証用のＩＤ及び第０世代の認証鍵（ＭＧ－ＩＤ／ＩＫ）をネットワークを介して提供しても良い。

【０２６９】つぎに、リッピング専用鍵をＥＭＤ鍵に鍵に更新して、ＥＭＤサーバ（Ｘ）４－３からダウンロードした音楽コンテンツを取り扱えるようにする処理の手順について説明する。

【０２７０】包括管理ユニット（Ｘ）３１５は、図２７又は図２８に示した手順により、ＣＤ－ＲＯＭ等のリムーバブルメディアやインターネット等のネットワークを介して提供され、パーソナルコンピュータ１内のＨＤＤ２１にインストールされている。このとき包括管理ユニット（Ｘ）３１５は、リッピング専用である第０世代のマスター鍵（ＯＭＧ－ＭＫ［０］）と、認証用のＩＤ及び第０世代の認証鍵（ＭＧ－ＩＤ／ＩＫ［０］）とを保

持しており、ポータブルデバイス（Ｘ）６－３の鍵の世代もデフォルトのままである。

【０２７１】まず、パーソナルコンピュータ１は、図２９に示すように、ユーザＩＤ及びパスワードを用いてネットワーク上のＥＭＤ登録サーバ３にアクセスをする（ステップＳ３１）。続いて、ＥＭＤ登録サーバ３は、ユーザＩＤ及びパスワードの認証を行う（ステップＳ３２）。続いて、認証に問題がなければ、ＥＭＤ登録サーバ３は、パーソナルコンピュータ１のＩＤ情報（ＯＭＧ－ＩＤ）を登録し、包括管理ユニット（Ｘ）３１５がＥＭＤサーバ（Ｘ）４－３と接続するための公開鍵（ＯＭＧ－ＰＫ）、秘密鍵（ＯＭＧ－ＫＳ）及び公開鍵の認証書（Ｃｅｒｔ［ＰＫ］）を生成する（ステップＳ３３）。続いて、ＥＭＤ登録サーバ３は、生成した公開鍵（ＯＭＧ－ＰＫ）、秘密鍵（ＯＭＧ－ＫＳ）及び公開鍵の認証書（Ｃｅｒｔ［ＰＫ］）を、パーソナルコンピュータ１に送信する（ステップＳ３４）。

【０２７２】続いて、ＥＭＤ登録サーバ３は、ポータブルデバイス（Ｘ）６－３のＩＤ情報（ＭＧ－ＩＤ），第ｉ世代の認証鍵（ＭＧ－ＩＫ［ｉ］），第ｉ世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ］）をパーソナルコンピュータ１に送信する（ステップＳ３５）。続いて、パーソナルコンピュータ１の包括管理ユニット（Ｘ）３１５は、受信したＩＤ情報（ＭＧ－ＩＤ），第ｉ世代の認証鍵（ＭＧ－ＩＫ［ｉ］），第ｉ世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ］）に基づき、これらの鍵を第ｉ世代に世代更新する（ステップＳ３６）。続いて、包括管理ユニット（Ｘ）３１５は、ポータブルデバイス（Ｘ）６－３との間で認証を行う（ステップＳ３７）。ポータブルデバイス（Ｘ）６－３は、認証がされると、自己の鍵の世代を第ｉ世代に更新する（ステップＳ３８）。

【０２７３】このことによって、包括管理ユニット（Ｘ）３１５は、音楽ＣＤ３６３等により提供される音楽コンテンツを、パーソナルコンピュータ１のハードディスク内に格納することができるとともに、ＥＭＤサーバ（Ｘ）４－３からダウロードした音楽コンテンツをパーソナルコンピュータ１のＨＤＤ２１に格納することができるようになる。

【０２７４】つぎに、ＥＭＤ鍵等の世代更新をする手順について説明する。

【０２７５】包括管理ユニット（Ｘ）３１５は、第ｉ世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ］）と、認証用のＩＤ及び第０世代の認証鍵（ＭＧ－ＩＤ／ＩＫ［ｉ］）とを保持しており、ポータブルデバイス（Ｘ）６－３の鍵の世代も第ｉ世代となっている。

【０２７６】まず、図３０に示すように、パーソナルコンピュータ１が何らかの処理のため、ＥＭＤ登録サーバ３にアクセスすると、ＥＭＤ登録サーバ３は、包括管理ユニット（Ｘ）３１５のＩＤを認証して、第（ｉ＋ｋ）世代の認証鍵（ＭＧ－ＩＫ［ｉ＋ｋ］）及び第（ｉ＋ｋ）世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ＋ｋ］）をパーソナルコンピュータ１に送信する（ステップＳ４１）。続いて、パーソナルコンピュータ１の包括管理ユニット（Ｘ）３１５は、受信した認証鍵及びマスター鍵を、第（ｉ＋ｋ）世代に更新する（ステップＳ４２）。続いて、包括管理ユニット（Ｘ）３１５は、ポータブルデバイス（Ｘ）６－３と認証を行う（ステップＳ４３）。ポータブルデバイス（Ｘ）６－３は、認証がされると、自己の鍵の世代を第ｉ世代から第（ｉ＋ｋ）世代に更新する（ステップＳ４４）。

【０２７７】また、図３１に示すように、一方、ポータブルデバイス（Ｘ）６－３が用いている認証鍵等の世代が第（ｉ＋ｋ）世代となっており、包括管理ユニット（Ｘ）３１５が保持している認証鍵等の世代が第ｉ世代となっている場合には、ポータブルデバイス（Ｘ）６－３と包括管理ユニット（Ｘ）３１５との認証が行われると、認証失敗となる（ステップＳ５１）。認証を失敗すると、包括管理ユニット（Ｘ）３１５は、ＥＭＤ登録サーバ３に対して、鍵要求を行う（ステップＳ５２）。鍵要求があると、ＥＭＤ登録サーバ３は、包括管理ユニット（Ｘ）３１５のＩＤを認証して、第（ｉ＋ｋ）世代の認証鍵（ＭＧ－ＩＫ［ｉ＋ｋ］）及び第（ｉ＋ｋ）世代のマスター鍵（ＯＭＧ－ＭＫ［ｉ＋ｋ］）を送信する（ステップＳ５３）。続いて、包括管理ユニット（Ｘ）３１５は、受信した認証鍵及びマスター鍵を、第（ｉ＋ｋ）世代に更新する（ステップＳ５４）。続いて、包括管理ユニット（Ｘ）３１５は、ポータブルデバイス（Ｘ）６－３と認証を行う（ステップＳ５５）。

【０２７８】このことによって、包括管理ユニット（Ｘ）３１５は、音楽ＣＤ３６３等により提供される音楽コンテンツを、パーソナルコンピュータ１のハードディスク内に格納することができるとともに、ＥＭＤサーバ（Ｘ）４－３からダウンロードした音楽コンテンツをパーソナルコンピュータ１のＨＤＤ２１に格納することができるようになる（ステップＳ３８）。

【０２７９】以上のように、音楽コンテンツ配信システムでは、包括管理ユニット（Ｘ）３１５及びポータブルデバイス（Ｘ）６－３が用いるマスター鍵及び認証鍵を、リッピング専用の鍵とサーバ接続鍵とに分け、さらに、サーバ接続鍵をネットワークを介してダウンロードするようにしている。このため、音楽コンテンツ配信システムでは、サーバから配信された音楽コンテンツの安全性が高まり、例えば、リッピング専用の鍵が破られたとしても、サーバからダウンロードされる音楽コンテンツを破ることができない。

【０２８０】また、音楽コンテンツ配信システムでは、包括管理ユニット（Ｘ）３１５及びポータブルデバイス（Ｘ）６－３が用いるマスター鍵及び認証鍵を、世代更新させて用いている。さらに、包括管理ユニット（Ｘ）３１５は、マスター鍵及び認証鍵がネットワークを介し

て供給され、世代更新を行う。このため、音楽コンテンツの安全性が高まる。

【０２８１】

【発明の効果】本発明によれば、データ処理装置が、コンテンツサーバから再取得した使用ログ情報に基づき、バックアップの復元又は再配信されたコンテンツデータの再生及び／又は制御を行う。

【０２８２】このことにより、本発明では、ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態の音楽コンテンツ配信システムの構成を示す図である。

【図２】上記音楽コンテンツ配信システムにおけるパーソナルコンピュータの構成を示す図である。

【図３】上記音楽コンテンツ配信システムにおけるポータブルデバイスの構成を示す図である。

【図４】上記パーソナルコンピュータの機能について説明する図である。

【図５】表示操作指示ウィンドウの一例を示す図である。

【図６】録音プログラムがディスプレイに表示させる表示例を示す図である。

【図７】上記音楽コンテンツ配信システムにおける、配信業者毎にフォーマットが異なるコンテンツの統一的な取り扱いについて説明するための図である。

【図８】統一転送プロトコルレイヤとアプリケーションレイヤとの関係を説明する図である。

【図９】一般的に用いられる利用条件情報のフォーマットを説明する図である。

【図１０】包括管理ユニットで用いられる統一利用条件情報を構成するファイルを説明する図である。

【図１１】上記統一利用条件情報のオートマトンファイルの構成を説明する図である。

【図１２】上記オートマトンファイルのオートマトン記述部に記述される音楽コンテンツの動作遷移を示すオートマトンの一例を説明する図である。

【図１３】上記オートマトンをｔｕｐｌｅ列で表現した図である。

【図１４】上記オートマトン記述部の構成を説明する図である。

【図１５】ＸＭＬの仕様に基づいて規定されたＤＴＤで定義されているイベントとコマンドとを示す図である。

【図１６】上記オートマトン記述部の第１の記述例を示す図である。

【図１７】上記第１の記述例の状態遷移図である。

【図１８】上記オートマトン記述部の第２の記述例を示す図である。

【図１９】上記第２の記述例の状態遷移図である。

【図２０】上記オートマトン記述部の第３の記述例を示す図である。

【図２１】上記第３の記述例の状態遷移図である。

【図２２】上記オートマトン記述部の第４の記述例を示す図である。

【図２３】上記統一利用条件情報のパラメータファイルの構成を説明する図である。

【図２４】上記パラメータファイルを更新した場合の構成を説明する図である。

【図２５】上記パラメータファイルのパラメータ記述部の構成を説明する図である。

【図２６】上記包括管理ユニットによるコンテンツの管理方法について説明する図である。

【図２７】包括管理ユニットがＣＤ－ＲＯＭからインストールされる場合の処理手順について説明する図である。

【図２８】包括管理ユニットがネットワークからダウンロードされてインストールされる場合の処理手順について説明する図である。

【図２９】リッピング鍵からＥＭＤ鍵に更新する更新手順について説明する図である。

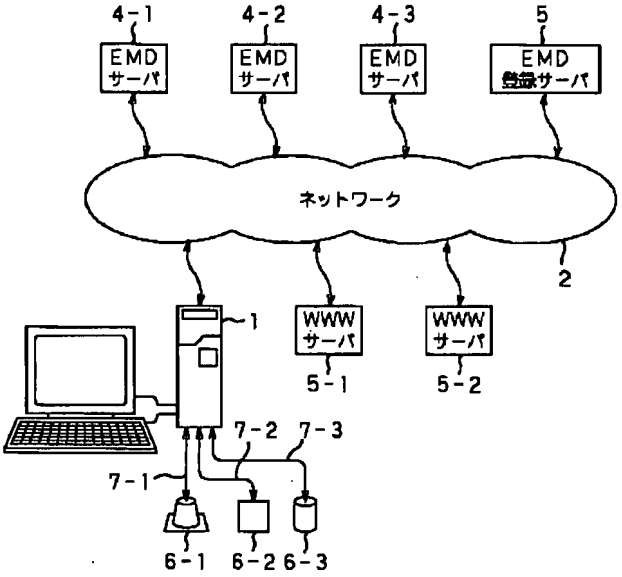
【図３０】ＥＭＤ鍵を更新する手順の第１の例について説明する図である。

【図３１】ＥＭＤ鍵を更新する手順の第２の例について説明する図である。

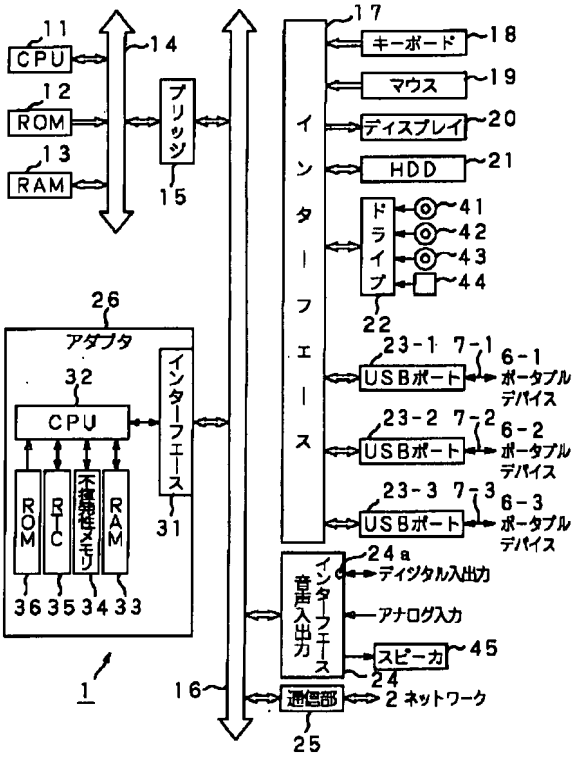
【符号の説明】

１　パーソナルコンピュータ、２　ネットワーク、３　ＥＭＤ登録サーバ、４ＥＭＤサーバ、６　ポータブルデバイス、７　ＵＳＢインターフェース、２１ハードディスク、３１１，３１２　再生用アプリケーション、３１３，３１４デバイスドライバ、３１５　包括管理ユニット、３１６　ＥＭＤ用受信インターフェース、３１７　ＥＭＤ用送信インターフェース、３１８　ＰＤドライバ

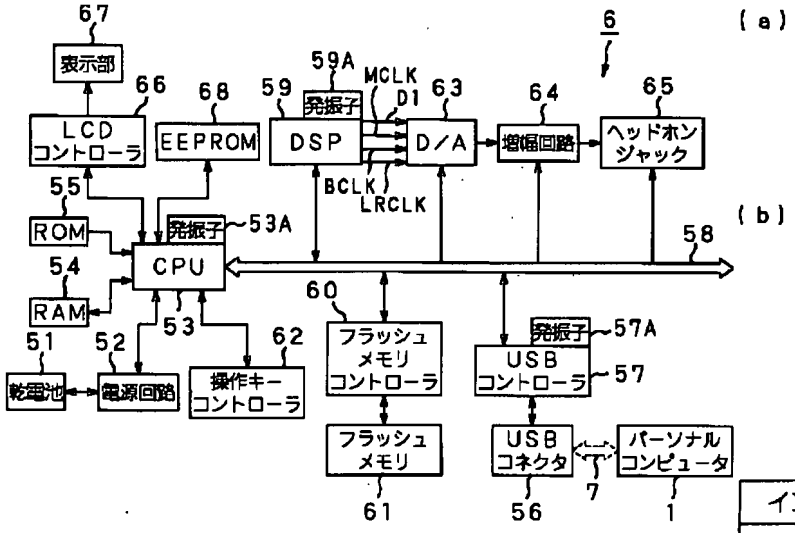
【図１】



【図２】



【図３】



【図９】

(a)

ポリシー	値
from	99/10/25
to	99/11/24
pay/play	yes/10円

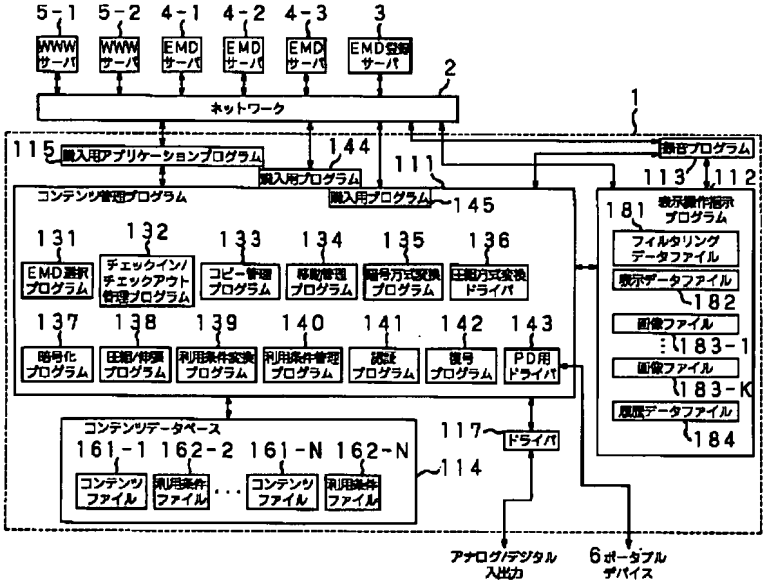
(b)

コンテンツ
利用条件情報

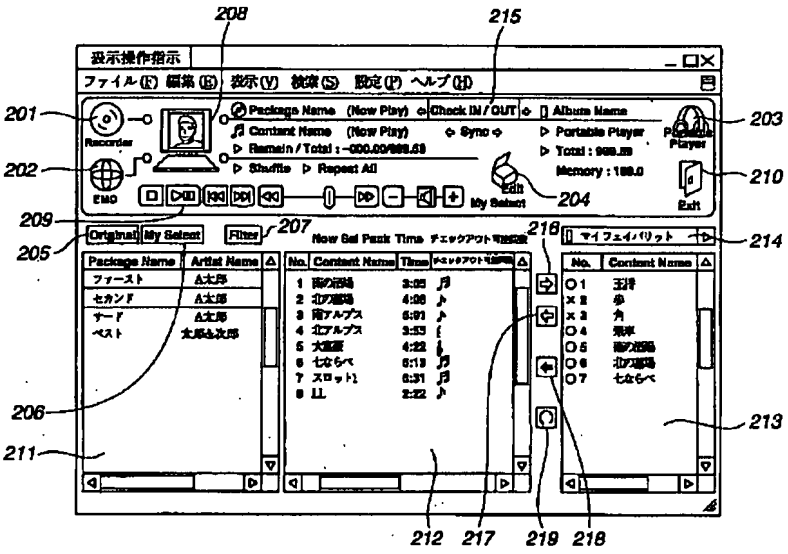
【図１０】

インデックスファイル	331
オートマトンファイル	332
パラメータファイル	333
履歴ファイル	334

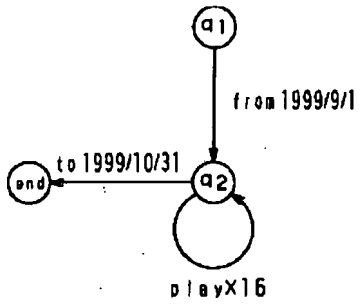
【図４】



【図５】



【図２１】



【図１１】

Automaton	341
MAC_{Kc}(Automaton)	342
$Sig_{K_E^{-1}}$(Automaton)	343
Cert(K_E^1)	344

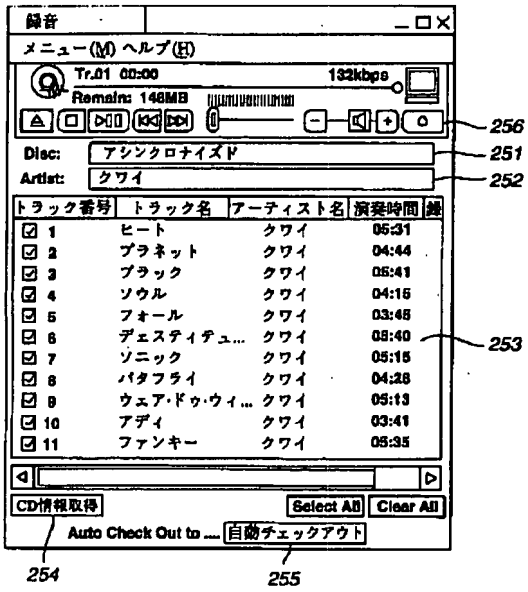
【図１３】

```
⟨q1,pay10,q2⟩
⟨q1,a.pay1000,q3⟩
⟨q1,pay(10×n),q4⟩
⟨q2,play,q1⟩
⟨q3,play,q3⟩
⟨q4,play×n,q4⟩
⟨q4,ε,q1⟩
⟨q5,pay100,q6⟩
⟨q5,a.pay2000,q7⟩
⟨q6,copy,q5⟩
⟨q7,copy,q7⟩
⟨q8,play,q8⟩
⟨q8,copy,q9⟩
```

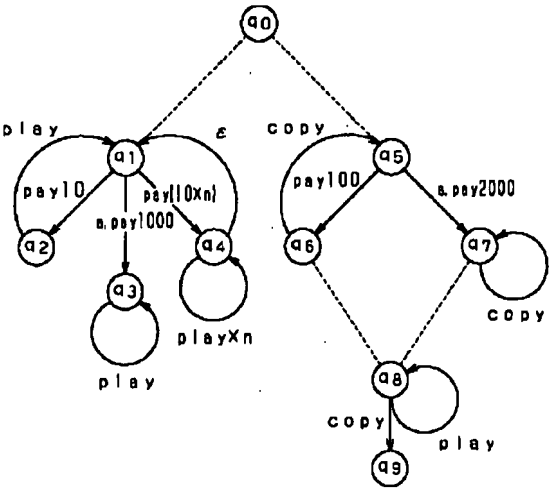
【図１５】

```
⟨!ENTITY % event" (
    play                    |
    copy                    |
    pay-for-play            |
    pay-for-copy            |
    pay-for-album-play      |
    pay-for-album-copy      |
    from                    |
    to                      |
    null
)")

⟨!ENTITY % command" (
    drop                    |
    dup                     |
    swap                    |
    add                     |
    subtract                |
    multiply                |
    divide                  |
    remainder               |
    upper                   |
    lower                   |
    equal                   |
    less                    |
    greater                 |
    less-equal              |
    greater-equal           |
    and                     |
    or                      |
    not                     |
    bit-and                 |
    bit-or                  |
    bit-xor                 |
    bit-not
)")
```

【図６】



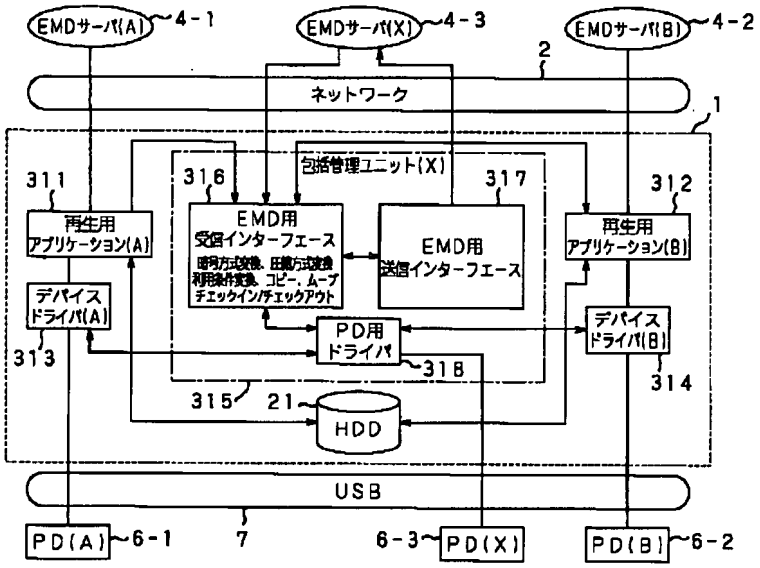
【図１２】

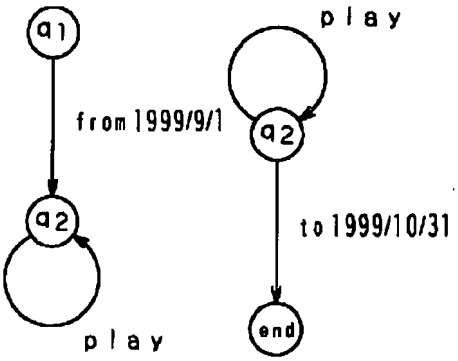


【図１７】

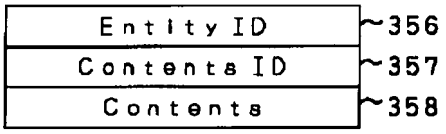
【図１９】

【図７】

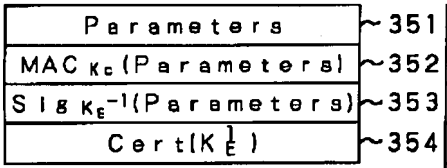




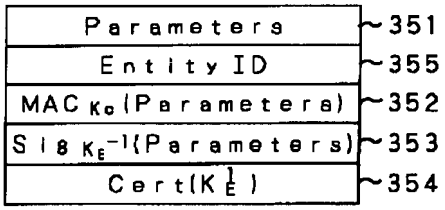
【図２５】



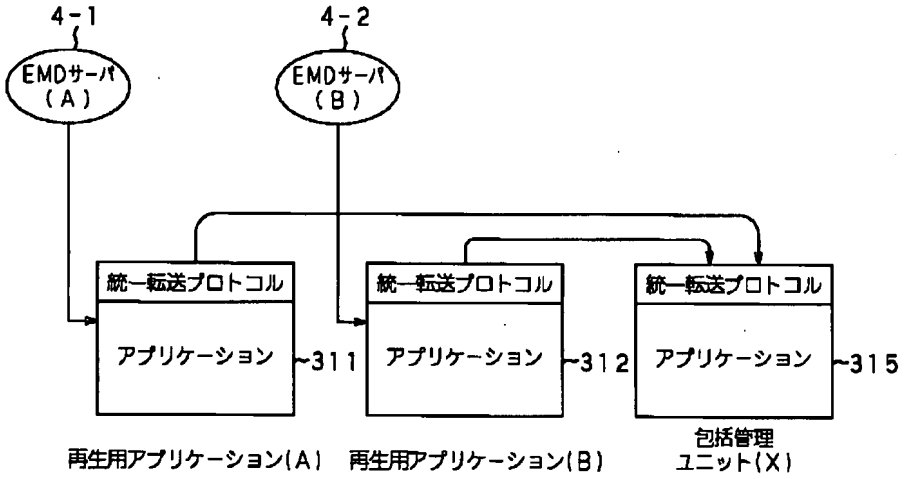
【図２３】



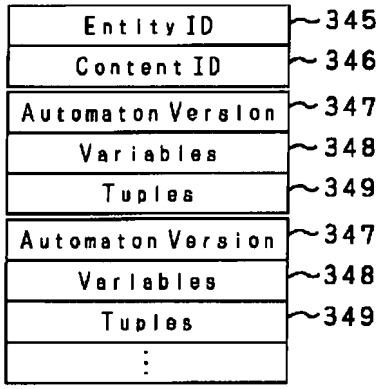
【図２４】



【図８】



【図１４】



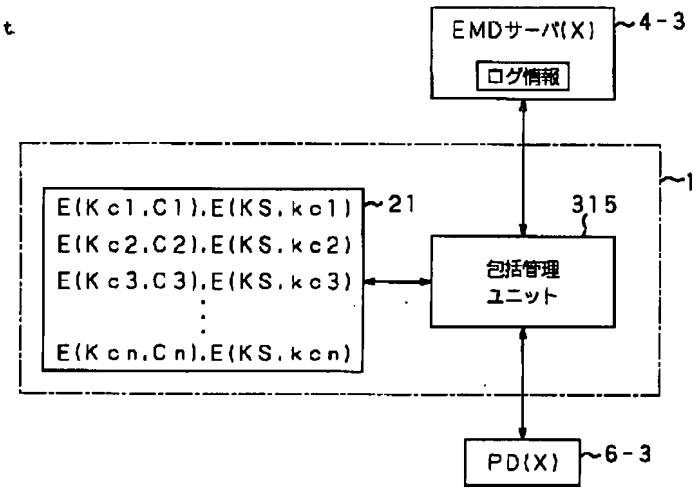
【図１６】

```
Content playable from 1999/9/1
⟨automaton⟩
  ⟨!—This usage rule system has one Right Unit.
   Initial state is q1--⟩
  ⟨initial-right-unit state="q1"/⟩

  ⟨node state="q1"⟩
    ⟨!—If after 1999/9/1, transfer to q2--⟩
    ⟨rule event="from" next-state="q2"⟩
      ⟨arguments⟩
        ⟨integer value="time:19990901"/⟩
      ⟨/arguments⟩
    ⟨/rule⟩
  ⟨/node⟩

  ⟨node state="q2"⟩
    ⟨!--Playable--⟩
    ⟨rule event="play" next-state="q2"/⟩
  ⟨/node⟩

⟨/automaton⟩
```

【図１８】

```
Content playable unil 1999/10/31
⟨automaton⟩
  ⟨!--This Usage Rule System has one Right Unit.
   Initial state is q2--⟩
  ⟨initial-right-unit state="q2"/⟩

  ⟨node state="q2"⟩
    ⟨!—If after 1999/10/31, transfer to end--⟩
    ⟨rule event="to" next-state="end"⟩
      ⟨arguments⟩
        ⟨integer value="time:19991031"/⟩
      ⟨/arguments⟩
    ⟨/rule⟩

    ⟨!--Playable--⟩
    ⟨rule event="play" next-state="q2"⟩
    ⟨/rule⟩
  ⟨/node⟩

  ⟨!—Unusable state--⟩
  ⟨node state="end"/⟩

⟨/automaton⟩
```

【図２６】



【図２０】

Content playable 16times 1999/9/1 to 1999/10/31

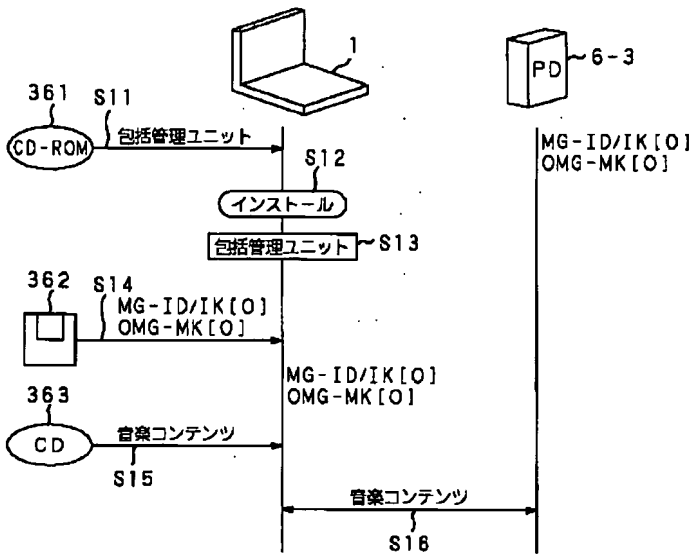
```
(automaton)

  (!-Defins counter variables for playable numbers. Initial value is 16--)
  (define-variable name="count" initial-value="16"/)

  (!-This Usage Rule System has one Right Unit. Initial state is q1--)
  (initial-right-unit state="q1"/)

  (node state="q1")
    (!-From 1999/9/1 transfer to q2--)
    (rule event="from" next-state="q2)
      (arguments)
        (integer value="time:19990901"/)
      (/arguments)
    (/rule)
  (/node)

  (node state="q2")
    (!-From 1999/10/31 transfer to end--)
    (rule event="to" next-state="end")
      (arguments)
        (integer value="time:19991031"/)
      (/arguments)
    (/rule)

    (rule event="play" next-state="q2")
      (!-playable only for "count" numbers--)
      (arguments)
        (variable name="count"/)
        (command name="load"/)
      (/arguments)
      (!-If this rule is selected, the "count" number decrements by one--)
      (action)
        (variable name="count"/)
        (command name="load"/)
        (integer value="1"/)
        (command name="subtract"/)
        (variable name="count"/)
        (command name="store"/)
      (/action)
    (/rule)
  (/node)

  (!-Unusable state--)
  (node state="end"/)

(/automaton)
```

【図２２】

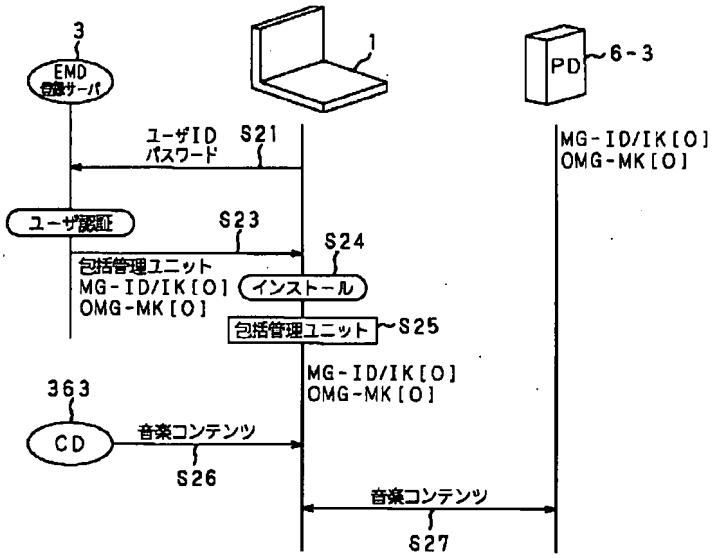
Content playable less than and/or equal to 16times

```
(automaton)

  (!-Define valuable counter for playable numbers
   Initial value is 16--)
  (define-variable name="count" initial-value="16"/)

  (!--Usage Rule System has one Right Unit
   Initial state is q2--)
  (initial-right-unit state="q1"/)

  (node state="q2")
    (rule event="play" next-state="q2")
      (!-"Count" number of times playable--)
      (arguments)
        (variable name="count"/)
        (command name="load"/)
      (/arguments)
      (!-If this rule is selected, "count"
       number decrements by one--)
      (action)
        (variable name="count"/)
        (command name="load"/)
        (integer value "1"/)
        (command name="subtract"/)
        (variable name="count"/)
        (command name="store"/)
      (/action)
    (/rule)
  (/node)

(/automaton)
```

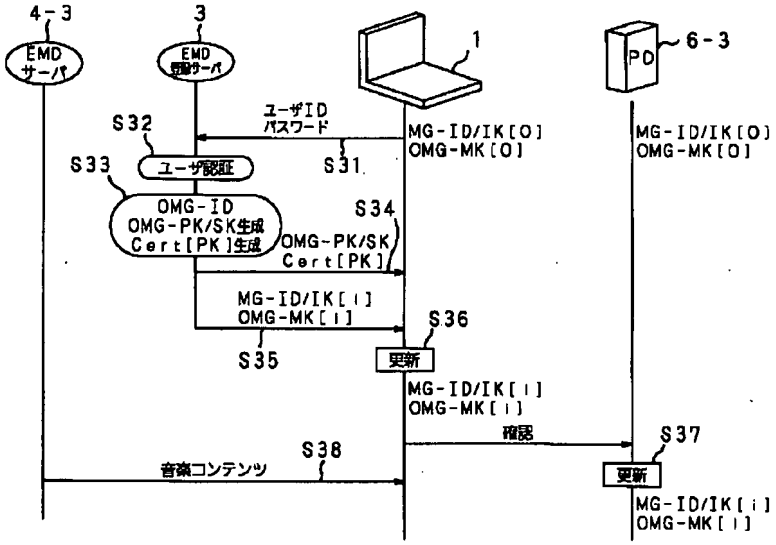
【図２７】



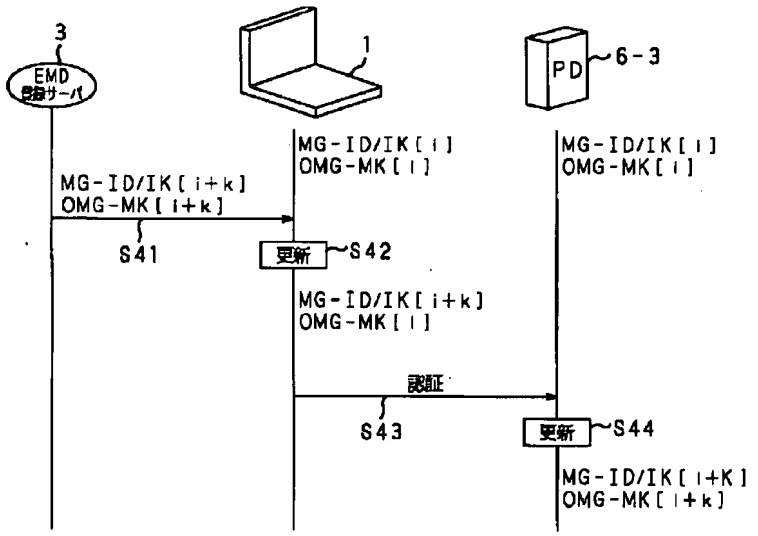
【図２８】


3
EMD
1
PD
6-3
ユーザID
パスワード
S21
MG-ID/IK[O]
OMG-MK[O]
ユーザ認証
S23
S24
包括管理ユニット
MG-ID/IK[O]
OMG-MK[O]
インストール
包括管理ユニット
S25
MG-ID/IK[O]
OMG-MK[O]
363
CD
音楽コンテンツ
S26
音楽コンテンツ
S27

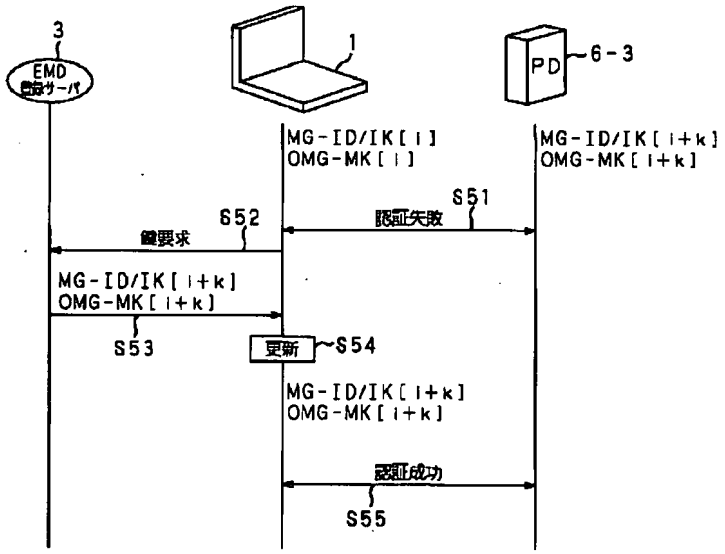
【図２９】


4-3
EMD
サーバ
3
EMD
1
PD
6-3
ユーザID
パスワード
S32
MG-ID/IK[O]
OMG-MK[O]
MG-ID/IK[O]
OMG-MK[O]
S33
ユーザ認証
S31
OMG-ID
OMG-PK/SK生成
Cert[PK]生成
S34
OMG-PK/SK
Cert[PK]
MG-ID/IK[i]
OMG-MK[i]
S36
S35
更新
MG-ID/IK[i]
OMG-MK[i]
暗号
S37
S38
音楽コンテンツ
更新
MG-ID/IK[i]
OMG-MK[i]

【図３０】



【図３１】



フロントページの続き

(72)発明者　田辺　充
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　江面　裕一
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　佐藤　一郎
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　海老原　宗毅
東京都品川区北品川６丁目７番35号　ソニー株式会社内

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成１９年５月２４日（２００７．５．２４）

【公開番号】特開２００１－１９５５０９（Ｐ２００１－１９５５０９Ａ）
【公開日】平成１３年７月１９日（２００１．７．１９）
【出願番号】特願２０００－３２６１２５（Ｐ２０００－３２６１２５）
【国際特許分類】
　Ｇ０６Ｑ　30/00　　(2006.01)
　Ｇ１０Ｋ　15/02　　(2006.01)
【ＦＩ】
　Ｇ０６Ｆ 17/60　　302 Ｅ
　Ｇ１０Ｋ 15/02

【手続補正書】
【提出日】平成１９年３月２８日（２００７．３．２８）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正の内容】
【発明の名称】コンテンツ提供システム、コンテンツ配信方法、記憶媒体、データ処理装置、及び、コテンツサーバ
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】　コンテンツデータをネットワークを介して配信するコンテンツサーバと、
　コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、
　上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすること
　を特徴とするコンテンツ提供システム。
【請求項２】　コンテンツデータをネットワークを介して配信するコンテンツサーバと、
　コンテンツデータの再生及び／又は制御をする再生制御プログラムを有し、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信するデータ処理装置とを備え、
　上記データ処理装置は、上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすること
　を特徴とするコンテンツ提供システム。

【請求項３】　コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、
　上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、
　上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに、配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、
　上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
　上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、上記使用ログ情報を上記データ処理装置に送信し、
　上記データ処理装置が、上記使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすること
　を特徴とするコンテンツ配信方法。
【請求項４】　コンテンツデータの再生及び／又は制御をする再生制御プログラムを有するデータ処理装置と、コンテンツデータをネットワークを介して上記データ処理装置に配信するコンテンツサーバとの間で行われるコンテンツ配信方法において、
　上記コンテンツサーバが、コンテンツデータを上記データ処理装置に配信し、
　上記データ処理装置が、上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、
　上記データ処理装置が、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
　上記データ処理装置が上記記憶媒体からコンテンツデータが取得できなくなったときには、上記コンテンツサーバが、この取得できなくなったコンテンツデータを上記データ処理装置に再配信するとともに、上記使用ログ情報を上記データ処理装置に送信し、
　上記データ処理装置が、上記使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすること
　を特徴とするコンテンツ配信方法。
【請求項５】　データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、
　上記再生制御プログラムは、
　上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をするとともに配信されたコンテンツデータのバックアップデータを記憶媒体に記憶し、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
　上記記憶媒体からコンテンツデータが取得できなくなったときには、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて上記記憶媒体に記憶しているコンテンツデータのバックアップデータの再生及び／又は制御をすること
　を特徴とする記憶媒体。
【請求項６】　データ処理装置にインストールされ、ネットワークを介してコンテンツサーバから配信されたコンテンツデータを取得し、このコンテンツデータの再生及び／又は制御をする再生制御プログラムが格納された記憶媒体であって、
　上記再生制御プログラムは、
　上記コンテンツサーバから配信されたコンテンツデータを記憶媒体に記憶して再生及び／又は制御をし、上記コンテンツデータの使用ログ情報を上記コンテンツサーバに送信し、
　上記記憶媒体からコンテンツデータが取得できなくなったときには、この取得できなくなったコンテンツデータを上記コンテンツサーバから再配信を受けるとともに、上記使用ログ情報を上記コンテンツサーバから取得し、この使用ログ情報に応じて再配信されたコンテンツデータの再生及び／又は制御をすること

を特徴とする記憶媒体。

【請求項７】　コンテンツサーバとネットワークを介して接続されたデータ処理装置であって、

上記コンテンツサーバとの間でデータを送受信する通信手段と、

コンテンツデータを記憶する記憶手段と、

上記記憶手段に記憶されたコンテンツデータを再生する再生手段と、

上記記憶手段に記憶されたコンテンツデータのコンテンツＩＤリストを含むログ情報を管理し、上記コンテンツサーバへ上記ログ情報を上記通信手段が送信するよう制御し、上記再生手段が上記コンテンツデータを再生するよう制御する制御手段と

を有し、

上記記憶手段に記憶された上記コンテンツデータが上記再生手段で再生できなくなったときは、上記通信手段が上記ログ情報に基づいて上記コンテンツサーバが送信するデータを受信すること

を特徴とするデータ処理装置。

【請求項８】　上記コンテンツサーバが送信するデータは、コンテンツデータであり、上記再生手段は、上記通信手段が受信したコンテンツデータを再生することを特徴とする請求項７記載のデータ処理装置。

【請求項９】　上記コンテンツデータは、コンテンツ鍵で暗号化されており、上記記憶手段は、コンテンツを暗号化したコンテンツ鍵を記憶しており、上記再生手段は上記コンテンツデータを上記コンテンツ鍵で復号化して再生し、上記コンテンツサーバが送信するデータは、コンテンツ鍵であることを特徴とする請求項７記載のデータ処理装置。

【請求項１０】　上記制御手段は、上記記憶手段に記憶されたコンテンツデータのバックアップデータを記録媒体に記憶するよう制御することを特徴とする請求項７記載のデータ処理装置。

【請求項１１】　上記通信手段は、上記ログ情報に基づいて上記コンテンツサーバが送信する整合検証値データを受信し、上記制御手段は、上記再生手段がコンテンツデータを再生するときは上記整合検証値データに基づいてコンテンツＩＤの検証を行うよう制御することを特徴とする請求項７記載のデータ処理装置。

【請求項１２】　ネットワークを介してデータ処理装置と接続されたコンテンツサーバであって、

コンテンツデータを記憶する記憶手段と、

上記記憶手段に記憶されたコンテンツデータを上記データ処理装置へ送信する通信手段と、

上記データ処理装置から受信したコンテンツデータのコンテンツＩＤリストを含むログ情報を上記データ処理装置に対応付けて上記記憶手段に記憶し、上記データ処理装置から要求があった場合、上記通信手段が上記ログ情報に基づいてデータを上記データ処理装置へ送信するよう制御する制御手段と

を有するコンテンツサーバ。

【請求項１３】　上記コンテンツＩＤリストに基づいて送信するデータはコンテンツデータであり、上記制御手段は上記記憶手段に記憶されたコンテンツデータを上記通信手段が送信するよう制御することを特徴とする請求項１２記載のコンテンツサーバ。

【請求項１４】　上記コンテンツＩＤリストに基づいて送信するデータは、コンテンツを復号化するためのコンテンツ鍵であることを特徴とする請求項１２記載のコンテンツサーバ。

【請求項１５】　上記コンテンツＩＤリストに基づいて整合検証値データを生成する生成手段を有し、

上記制御手段は上記生成手段で生成した整合検証値データを上記データ処理装置へ送信するよう前記通信手段を制御することを特徴とする請求項１２記載のコンテンツサーバ。

【手続補正３】

【補正対象書類名】明細書

【補正対象項目名】０００１
【補正方法】変更
【補正の内容】
【０００１】
【発明の属する技術分野】
本発明は、ネットワークを介して音楽データ等のコンテンツデータを提供するコンテンツ提供システム、コンテンツ配信方法、記憶媒体、データ処理装置、及び、コンテンツサーバに関するものである。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００６
【補正方法】変更
【補正の内容】
【０００６】
本発明は、このような実情を鑑みてなされたものであり、ネットワークを介してコンテンツ配信したコンテンツデータが、一旦破壊されてしまった場合であっても、著作権の保護を図りながら、コンテンツデータを復元することができるコンテンツ提供システム、コンテンツ配信方法、記憶媒体、データ処理装置、及び、コンテンツサーバを提供することを目的とする。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１８
【補正方法】変更
【補正の内容】
【００１８】
この記憶媒体では、再生制御プログラムがインストールされたデータ処理装置に対して、コンテンツサーバから再取得した使用ログ情報に基づき、再配信されたコンテンツデータの再生及び／又は制御を行わせる。
本発明にかかるデータ処理装置は、コンテンツサーバとネットワークを介して接続されたデータ処理装置であって、上記コンテンツサーバとの間でデータを送受信する通信手段と、コンテンツデータを記憶する記憶手段と、上記記憶手段に記憶されたコンテンツデータを再生する再生手段と、上記記憶手段に記憶されたコンテンツデータのコンテンツＩＤリストを含むログ情報を管理し、上記コンテンツサーバへ上記ログ情報を上記通信手段が送信するよう制御し、上記再生手段が上記コンテンツデータを再生するよう制御する制御手段とを有し、上記記憶手段に記憶された上記コンテンツデータが上記再生手段で再生できなくなったときは、上記通信手段が上記ログ情報に基づいて上記コンテンツサーバが送信するデータを受信することを特徴とする。
このデータ処理装置は、ログ情報に基づいてコンテンツサーバから再配信されたコンテンツデータを受信する。
本発明にかかるコンテンツサーバは、ネットワークを介してデータ処理装置と接続されたコンテンツサーバであって、コンテンツデータを記憶する記憶手段と、上記記憶手段に記憶されたコンテンツデータを上記データ処理装置へ送信する通信手段と、上記データ処理装置から受信したコンテンツデータのコンテンツＩＤリストを含むログ情報を上記データ処理装置に対応付けて上記記憶手段に記憶し、上記データ処理装置から要求があった場合、上記通信手段が上記ログ情報に基づいてデータを上記データ処理装置へ送信するよう制御する制御手段とを有することを特徴とする。
このコンテンツサーバは、データ処理装置から受信したログ情報をデータ処理装置に対応付けて記憶し、このログ情報に基づいてデータ処理装置にデータを送信する。

PATENT ABSTRACTS OF JAPAN
(11)Publication number : 2001-195509
(43)Date of publication of application : 19.07.2001
(51)Int.Cl. G06F 17/60
G10K 15/02
(21)Application number : 2000-326125 (71)Applicant : SONY CORP
(22)Date of filing : 25.10.2000 (72)Inventor : ISHIGURO RYUJI
KAWAKAMI TATSU
TANABE MITSURU
EOMO YUICHI
SATO ICHIRO
EBIHARA SHUGI
(30)Priority
Priority number : 11303138
Priority date : 25.10.1999
Priority country : JP
(54) CONTENTS PROVIDING SYSTEM, CONTENTS DISTRIBUTING METHOD, AND STORAGE MEDIUM
(57)Abstract:
PROBLEM TO BE SOLVED: To restore contents data while protecting a copyright even when the contents data distributed through a network are temporarily destroyed.
SOLUTION: A PC stores the backup of distributed music contents on a hard disk and transmits the use log information on the music contents stored on the hard disk to an EMD server. When the music contents on the hard disk are destroyed, for example, the PC acquires the use log information from the EMD server and reproduces the backup data stored on the hard disk corresponding to the use log information.
LEGAL STATUS [Date of request for examination] 28.03.2007
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS
[Claim(s)]

[Claim 1] The contents server which distributes contents data through a network, It has the playback control program which carries out playback and/or control of contents data. Memorize to a storage the contents data distributed from the above-mentioned contents server, and the backup data of the contents data distributed while carrying out playback and/or control are memorized to a storage. It has the data processor which transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. The above-mentioned data processor When it becomes impossible to acquire contents data from the above-mentioned storage The contents offer system characterized by carrying out the playback and/or control of backup data of contents data which acquired the above-mentioned use log information from the above-mentioned contents server, and have been memorized to the above-mentioned storage according to this use log information.
[Claim 2] The contents server which distributes contents data through a network, It has the playback control program which carries out playback and/or control of contents data. Memorize to a storage the contents data distributed from the above-mentioned contents server, and playback and/or control are carried out. It has the data processor which transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. The above-mentioned data processor When it becomes impossible to acquire contents data from the above-mentioned storage While receiving re-distribution from the above-mentioned contents server, this contents data it became impossible to acquire The contents offer system characterized by carrying out playback and/or control of the contents data which acquired the above-mentioned use log information from the above-mentioned contents server, and were re-distributed according to this use log information.
[Claim 3] The data processor which has the playback control program which carries out playback and/or control of contents data, In the contents distribution approach performed between the contents servers which distribute contents data to the above-mentioned data processor through a network While the above-mentioned contents server distributes contents data to the above-mentioned data processor, memorizing to a storage the contents data with which the above-mentioned data processor was distributed from the above-mentioned contents server and carrying out playback and/or control The backup data of the distributed contents data are memorized to a storage. The above-mentioned data processor transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. When it becomes impossible for the above-mentioned data processor to acquire contents data from the above-mentioned storage The contents distribution approach that the above-mentioned contents server transmits the above-mentioned use log information to the above-mentioned data processor, and the above-mentioned data processor is characterized by carrying out the playback and/or control of backup data of contents data which have been memorized to the above-mentioned storage according to the above-mentioned use log information.
[Claim 4] The data processor which has the playback control program which carries out playback and/or control of contents data, In the contents distribution approach performed between the contents servers which distribute contents data to the above-mentioned data processor through a network The above-mentioned contents server distributes contents data to the above-mentioned data processor. The above-mentioned

data processor memorizes to a storage the contents data distributed from the above-mentioned contents server, and carries out playback and/or control. The above-mentioned data processor transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. When it becomes impossible for the above-mentioned data processor to acquire contents data from the above-mentioned storage While re-distributing this contents data it became impossible to acquire to the above-mentioned data processor, the above-mentioned contents server The contents distribution approach that the above-mentioned use log information is transmitted to the above-mentioned data processor, and the above-mentioned data processor is characterized by carrying out playback and/or control of the contents data re-distributed according to the above-mentioned use log information.

[Claim 5] It is installed in a data processor and the contents data distributed from the contents server through the network are acquired. It is the storage with which the playback control program which carries out playback and/or control of this contents data was stored. The above-mentioned playback control program Memorize to a storage the contents data distributed from the above-mentioned contents server, and the backup data of the contents data distributed while carrying out playback and/or control are memorized to a storage. When the use log information of the above-mentioned contents data is transmitted to the above-mentioned contents server and it becomes impossible to acquire contents data from the above-mentioned storage The storage characterized by carrying out the playback and/or control of backup data of contents data which acquired the above-mentioned use log information from the above-mentioned contents server, and have been memorized to the above-mentioned storage according to this use log information.

[Claim 6] It is installed in a data processor and the contents data distributed from the contents server through the network are acquired. It is the storage with which the playback control program which carries out playback and/or control of this contents data was stored. The above-mentioned playback control program Memorize to a storage the contents data distributed from the above-mentioned contents server, and playback and/or control are carried out. When the use log information of the above-mentioned contents data is transmitted to the above-mentioned contents server and it becomes impossible to acquire contents data from the above-mentioned storage While receiving re-distribution from the above-mentioned contents server, this contents data it became impossible to acquire The storage characterized by carrying out playback and/or control of the contents data which acquired the above-mentioned use log information from the above-mentioned contents server, and were re-distributed according to this use log information.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the contents offer system and the contents distribution approach of offering contents data, such as music data, through a network, and a storage.

[0002]

[Description of the Prior Art] In recent years, online distribution of the music content using networks, such as the Internet and cable television, began to be put in practical use.
[0003] In the distribution system of such a music content, a contents distribution contractor offers a music content on Web, when distributing a music content through a network. Moreover, the user using this music distribution system accesses Web which a contents distribution contractor offers using a self personal computer, and downloads a desired music content.
[0004]
[Problem(s) to be Solved by the Invention] By the way, generally in such a music distribution system, accounting is carried out through a network as opposed to the downloaded music content.
[0005] However, if the data in the personal computer which a user holds break for example, the once purchased music content will also disappear. Therefore, in order to have restored the music content, contents had to be purchased again.
[0006] This invention is made in view of such the actual condition, and it aims at offering the contents offer system which can restore contents data, the contents distribution approach, and a storage, aiming at protection of copyright, even if the contents data which carried out contents distribution through the network are the case where it has once been destroyed.
[0007]
[Means for Solving the Problem] The contents server to which the contents offer system concerning this invention distributes contents data through a network, It has the playback control program which carries out playback and/or control of contents data. Memorize to a storage the contents data distributed from the above-mentioned contents server, and the backup data of the contents data distributed while carrying out playback and/or control are memorized to a storage. It has the data processor which transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. The above-mentioned data processor When it becomes impossible to acquire contents data from the above-mentioned storage The above-mentioned use log information is acquired from the above-mentioned contents server, and it is characterized by carrying out the playback and/or control of backup data of contents data which have been memorized to the above-mentioned storage according to this use log information.
[0008] In a contents offer system, a data processor performs playback and/or control of restoration data of backup based on the use log information re-acquired from the contents server.
[0009] In the contents offer system concerning this invention The contents server which distributes contents data through a network, It has the playback control program which carries out playback and/or control of contents data. Memorize to a storage the contents data distributed from the above-mentioned contents server, and playback and/or control are carried out. It has the data processor which transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. The above-mentioned data processor When it becomes impossible to acquire contents data from the above-mentioned storage While receiving re-distribution for this contents data it became impossible to acquire from the above-mentioned contents server, the above-

mentioned use log information is acquired from the above-mentioned contents server, and it is characterized by carrying out playback and/or control of the contents data re-distributed according to this use log information.
[0010] In this contents offer system, playback and/or control of the contents data with which the data processor was re-distributed based on the use log information re-acquired from the contents server are performed.
[0011] The data processor which has the playback control program with which the contents distribution approach concerning this invention carries out playback and/or control of contents data, In the contents distribution approach performed between the contents servers which distribute contents data to the above-mentioned data processor through a network While the above-mentioned contents server distributes contents data to the above-mentioned data processor, memorizing to a storage the contents data with which the above-mentioned data processor was distributed from the above-mentioned contents server and carrying out playback and/or control The backup data of the distributed contents data are memorized to a storage. The above-mentioned data processor transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. When it becomes impossible for the above-mentioned data processor to acquire contents data from the above-mentioned storage The above-mentioned contents server transmits the above-mentioned use log information to the above-mentioned data processor, and the above-mentioned data processor is characterized by carrying out the playback and/or control of backup data of contents data which have been memorized to the above-mentioned storage according to the above-mentioned use log information.
[0012] By this contents distribution approach, a data processor performs playback and/or control of restoration data of backup based on the use log information re-acquired from the contents server.
[0013] The data processor which has the playback control program with which the contents distribution approach concerning this invention carries out playback and/or control of contents data, In the contents distribution approach performed between the contents servers which distribute contents data to the above-mentioned data processor through a network The above-mentioned contents server distributes contents data to the above-mentioned data processor. The above-mentioned data processor memorizes to a storage the contents data distributed from the above-mentioned contents server, and carries out playback and/or control. The above-mentioned data processor transmits the use log information of the above-mentioned contents data to the above-mentioned contents server. When it becomes impossible for the above-mentioned data processor to acquire contents data from the above-mentioned storage While re-distributing this contents data it became impossible to acquire to the above-mentioned data processor, the above-mentioned contents server The above-mentioned use log information is transmitted to the above-mentioned data processor, and the above-mentioned data processor is characterized by carrying out playback and/or control of the contents data re-distributed according to the above-mentioned use log information.
[0014] By this contents distribution approach, playback and/or control of the contents data with which the data processor was re-distributed based on the use log information re-acquired from the contents server are performed.

[0015] The storage concerning this invention is installed in a data processor, and the contents data distributed from the contents server through the network are acquired. It is the storage with which the playback control program which carries out playback and/or control of this contents data was stored. The above-mentioned playback control program Memorize to a storage the contents data distributed from the above-mentioned contents server, and the backup data of the contents data distributed while carrying out playback and/or control are memorized to a storage. When the use log information of the above-mentioned contents data is transmitted to the above-mentioned contents server and it becomes impossible to acquire contents data from the above-mentioned storage The above-mentioned use log information is acquired from the above-mentioned contents server, and it is characterized by carrying out the playback and/or control of backup data of contents data which have been memorized to the above-mentioned storage according to this use log information.
[0016] Playback and/or control of restoration data of backup are made to perform in this storage to the data processor with which the playback control program was installed based on the use log information re-acquired from the contents server.
[0017] The storage concerning this invention is installed in a data processor, and the contents data distributed from the contents server through the network are acquired. It is the storage with which the playback control program which carries out playback and/or control of this contents data was stored. The above-mentioned playback control program Memorize to a storage the contents data distributed from the above-mentioned contents server, and playback and/or control are carried out. When the use log information of the above-mentioned contents data is transmitted to the above-mentioned contents server and it becomes impossible to acquire contents data from the above-mentioned storage While receiving re-distribution for this contents data it became impossible to acquire from the above-mentioned contents server, the above-mentioned use log information is acquired from the above-mentioned contents server, and it is characterized by carrying out playback and/or control of the contents data re-distributed according to this use log information.
[0018] Playback and/or control of the re-distributed contents data are made to perform in this storage to the data processor with which the playback control program was installed based on the use log information re-acquired from the contents server.
[0019]
[Embodiment of the Invention] It explains to a detail, referring to a drawing as a gestalt of the best operation of this invention hereafter about the music content distribution system which applied this invention. This music content distribution system is a system which performs management of the music content which downloaded to the personal computer or the portable device and was further downloaded from the server through the network, or the music content read in CD etc.
[0020] (1) The whole music content distribution system block diagram 1 is drawing showing the whole music content distribution system configuration which applied this invention.
[0021] This music content distribution system is equipped with a personal computer 1, the networks 2, such as the Internet and a Local Area Network, the registration server 3, two or more EMD (Electrical Music Distribution) servers 4 (4-1, 4-2, 4-3) that distribute music data (it is hereafter called contents.), and the WWW server 5 (5-1, 5-2), and is

constituted. Moreover, through the USB cable 7 (7-1, 7-2, 7-3), storages, such as memory card, are stored in the interior and the portable device 6 (6-1, 6-2, 6-3) which is the music regenerator machine of the pocket mold which reproduces contents is connected to a personal computer 1.

[0022] A personal computer 1 is connected with the EMD registration server 3, the EMD server 4 (4-1, 4-2, 4-3), and the WWW (World Wide Web) server 5 (5-1, 5-2) through a network 2.

[0023] From the EMD server 4 (4-1, 4-2, 4-3), a personal computer 1 receives the contents compressed by the predetermined compression method, and enciphers and records them with a predetermined cipher system. Moreover, a personal computer 1 compresses the contents read in CD (Compact Disc) etc. by the predetermined compression method, and enciphers and records them with a predetermined cipher system. As a compression method, methods, such as ATRAC (Adaptive Transform Acoustic Coding)3 (trademark) and MP3 (MPEG Audio Layer-3), are used, for example. Moreover, DES (Data Encryption Standard) etc. is used as a cipher system.

[0024] Moreover, when receiving distribution of contents, a personal computer 1 also receives distribution of the use condition information which shows the use conditions of the contents, and records it. Moreover, when recording the contents read in CD etc., according to the playback conditions of the contents, a personal computer 1 generates use condition information, and records it.

[0025] Moreover, a personal computer 1 updates use condition information corresponding to having recorded the contents currently enciphered and recorded on the portable device 6 (6-1, 6-2, 6-3), and having made them memorize with related information, such as use condition information and a music name, and a player, through the USB cable 7 (7-1, 7-2, 7-3). This processing is called check-out. Use condition information carries out 1 **** of the counts of the contents which the personal computer 1 is recording and which can be checked out, when you check out. Corresponding contents cannot be checked out when the count which can be checked out is 0.

[0026] Moreover, a personal computer 1 is made to respond to having eliminated and (or not using it and putting) eliminated the contents memorized by the portable device 6 (6-1, 6-2, 6-3) through the USB cable 7 (7-1, 7-2, 7-3), and updates use condition information. This elimination processing is called check-in. When you check in, 1 **** of the counts of the contents which the personal computer 1 is recording and which can be checked out is carried out.

[0027] In addition, to the contents which other personal computers checked out to the portable device 6, check-in cannot do a personal computer 1. That is, he can check in only at the contents which personal computer 1 self checked out.

[0028] When, as for the EMD registration server 3, a personal computer 1 starts acquisition of contents from the EMD server 4 (4-1, 4-2, 4-3), A network 2 is minded corresponding to the demand of a personal computer 1. While transmitting an authentication key required for the mutual recognition of a personal computer 1 and the EMD server 4 (4-1, 4-2, 4-3) to a personal computer 1 The program for connecting with the EMD server 4 (4-1, 4-2, 4-3) is transmitted to a personal computer 1.

[0029] The EMD server 4 (4-1, 4-2, 4-3) supplies contents to a personal computer 1 through a network 2 corresponding to the demand of a personal computer 1 with the

associated data (for example, a music name or a player etc.) of use condition information and contents.
[0030] The contents which each EMD server 4 (4-1, 4-2, 4-3) distributes are compressed by the method of predetermined compression. The compression methods may differ for every server. Moreover, the contents which each EMD server 4 (4-1, 4-2, 4-3) supplies are enciphered and distributed with a predetermined cipher system. The cipher systems may differ for every server.
[0031] The WWW server 5 (5-1, 5-2) supplies the data (for example, a music name or a composer name etc.) corresponding to the contents read in CDs (for example, the album name of CD or the selling firm of CD etc.) and CD which read contents to a personal computer 1 through a network 2 corresponding to the demand of a personal computer 1.
[0032] The portable device 6 (6-1, 6-2, 6-3) is equipment which is reproduced and outputs the contents (namely, checked-out contents) supplied from the personal computer 1 to the headphone which are not illustrated.
[0033] Each portable device 6 (6-1, 6-2, 6-3) has the storage for memorizing contents. As a storage, the IC memory in which removal with which the internal substrate of equipment was equipped is impossible, the memory card which can be detached and attached are used, for example. The portable device 6 (6-1, 6-2, 6-3) is connected with a personal computer 1 through the physical interfaces 7 (7-1, 7-2, 7-3), such as USB, and contents are transmitted. At this time, contents are transmitted in the condition of having been enciphered and compressed, and use condition information is also added.
[0034] Each portable device 6 (6-1, 6-2, 6-3) will be reproduced by reading the enciphered contents from a storage, if it is usually used where connection with a personal computer 1 is separated, and a playback instruction is given by the user in this condition. Moreover, based on the use condition information added to each contents, restrict playback, deletion of contents etc. is controlled, or each portable device 6 (6-1, 6-2, 6-3) performs renewal of use condition information etc. if needed.
[0035] Hereafter, when it is not necessary to distinguish the portable device 6-1, 6-2, and 6-3 separately, the portable device 6 is only called.
[0036] Next, the configuration of a personal computer 1 is explained with reference to drawing 2 .
[0037] CPU (Central Processing Unit)11 actually performs various application programs (for details, it mentions later.) and OS (Operating System). Generally ROM (Read-only Memory)12 stores the data of immobilization fundamentally of the parameters the program which CPU11 uses, and for an operation. RAM (Random Access Memory)13 stores a variable parameter suitably in the program used in activation of CPU11, and its activation. These are mutually connected by the host bus 14 which consists of CPU buses etc.
[0038] The host bus 14 minds a bridge 15 and is PCI (Peripheral ComponentInterconnect/Interface). It connects with the external buses 16, such as a bus.
[0039] A keyboard 18 is operated by the user when inputting various kinds of commands into CPU11. A mouse 19 is operated by the user when performing the directions and selection of the point on the screen of a display 20. A display 20 consists of a liquid crystal display or CRT (Cathode Ray Tube), and displays various information

in a text or an image. HDD (Hard Disk Drive) 21 drive a hard disk, and record or reproduce the program and information which are performed by CPU11 to them.
[0040] Drive 22 reads the data or the program currently recorded on the magnetic disk 41 with which it is equipped, an optical disk 42 (CD is included), a magneto-optic disk 43, or semiconductor memory 44, and supplies the data or program to RAM13 with which it connects through the interface 17, the external bus 16, the bridge 15, and the host bus 14.
[0041] The portable device 6 (6-1, 6-2, 6-3) is connected to the USB port 23 (23-1, 23-2, 23-3) through the USB cable 7 (7-1, 7-2, 7-3). The USB port 23 outputs the data (for example, the command of contents or the portable device 6 etc. is included) supplied from HDD21, CPU11, or RAM13 through an interface 17, an external bus 16, a bridge 15, or the host bus 14 to the portable device 6 (6-1, 6-2, 6-3).
[0042] The voice-input/output interface 24 which has IEC(Internationl Electrotechnical Commission) 60958 terminal 24a performs interface processing of digitized voice I/O or an analog voice input/output. A loudspeaker 45 outputs the predetermined voice corresponding to contents based on the sound signal supplied from the voice-input/output interface 24.
[0043] These keyboards 18, a mouse 19, a display 20, HDD21, the drive 22, the USB port 23, and the voice-input/output interface 24 are connected to the interface 17, and the interface 17 is connected to CPU11 through the external bus 16, the bridge 15, and the host bus 14.
[0044] A network 2 is connected and the communications department 25 stores in the packet of a predetermined method the data (for example, the demand of registration or the Request to Send of contents etc.) supplied from CPU11 or HDD21. While transmitting through a network 2, the data (for example, an authentication key or contents etc.) stored in the packet which received are outputted to CPU11, RAM13, or HDD21 through a network 2.
[0045] Formed in one as a semiconductor IC, CPU32 of the adapter 26 with which a personal computer 1 is equipped has two incomes with CPU11 of a personal computer 1 through an external bus 16, a bridge 15, and the host bus 14, and performs various kinds of processings. CPU32 performs various kinds of processings upwards, and RAM33 memorizes required data and a required program. Nonvolatile memory 34 memorizes the data which need to be held even after the power source of a personal computer 1 is turned off. When the program enciphered has been transmitted to ROM36 from the personal computer 1, the program which decodes it is memorized. RTC (Real Time Clock)35 -- a time check -- actuation is performed and time information is offered. The semiconductor IC is designed by the secure environment and has resistance to access malicious from the outside. In addition, this function may consist of software programs.
[0046] The communications department 25 and an adapter 26 are connected to CPU11 through the external bus 16, the bridge 15, and the host bus 14.
[0047] Next, the configuration of the portable device 6 is explained with reference to drawing 3 .
[0048] A power circuit 52 makes the portable device 6 whole drive by transforming into the internal power of a predetermined electrical potential difference the supply voltage supplied from a dry cell 51, and supplying CPU53 - a display 67.

[0049] The USB controller 57 supplies the data containing the contents transmitted from the personal computer 1 to CPU53 through an internal bus 58, when it connects with a personal computer 1 through the USB cable 7 through the USB connector 56.
[0050] The data transmitted from a personal computer 1 consist of 64 bytes per one packet of data, and are transmitted from a personal computer 1 at the transfer rate of 12 Mbit/sec.
[0051] The data transmitted to the portable device 6 consist of a header and contents. While content ID, a file name, header size, a contents key, a file size, Codec ID, file information, etc. are stored, use condition information required for playback limit processing etc. is stored in the header. Contents are encoded and enciphered by coding methods, such as ATRAC3.
[0052] Header size expresses the data lengths (for example, 33 etc. bytes etc.) of a header, and a file size expresses the data lengths (for example, 33,636,138 etc. bytes etc.) of contents.
[0053] A contents key is a key for decoding the contents enciphered, and is transmitted to the portable device 6 from a personal computer 1 in the condition of having been enciphered based on the session key (momentary key) generated by processing of the mutual recognition of a personal computer 1 and the portable device 6.
[0054] When the portable device 6 is connected to the USB port 23 of a personal computer 1 through the USB cable 7, the portable device 6 and a personal computer 1 perform processing of mutual recognition. Processing of this mutual recognition is processing of authentication of for example, a challenge response method. Incidentally, DSP59 of the portable device 6 performs processing of decryption (decode), when processing authentication of a challenge response method.
[0055] A challenge response method is a method which answers with the value (response) which the portable device 6 generated to a certain value (challenge) which a personal computer 1 generates using the private key currently shared with a personal computer 1. Since the value which a personal computer 1 generates changes for every processing of authentication in processing of the mutual recognition of a challenge response method each time, even if the value which the portable device 6 outputted and which was generated using the private key is read for example, and it receives the so-called attack of spoofing, since the values used for mutual recognition differ, by processing of the following mutual recognition, as for a personal computer 1, injustice is detectable.
[0056] Content ID is ID for specifying contents corresponding to contents.
[0057] Codec ID is ID corresponding to the coding method of contents, for example, codec ID"1" corresponds to ATRAC3, and codec ID"0" corresponds to MP3 (MPEG (Moving Picture Experts Group) Audio Layer-3).
[0058] A file name is ASCII (American National Standard Code for Information Interchange) about the contents file (it mentions later) which the personal computer 1 corresponding to contents is recording. It is data cconverted with the code and file information is data which changed the music name corresponding to contents, the artist name, the songwriter name, or the composer name into the ASCII code.
[0059] When the portable device 6 receives the write-in instruction of contents with contents from a personal computer 1, CPU53 which performs the main program read from RAM54 or ROM55 makes the contents which controlled reception and the flash

memory controller 60 and received the write-in instruction from the personal computer 1 write in a flash memory 61.
[0060] A flash memory 61 has the storage capacity of about 64 MByte(s), and memorizes contents. Moreover, the code for playback for elongating the contents compressed by the predetermined compression method is beforehand stored in the flash memory 61.
[0061] In addition, you may enable it to make a flash memory 61 removable as a memory card at the portable device 6.
[0062] When the playback instruction corresponding to depression actuation of the playback/earth switch which is not illustrated by the user is supplied to CPU53 through the actuation key controller 62, CPU53 makes the flash memory controller 60 read the code for playback, and contents, and DSP59 is made to transmit it to it from a flash memory 61.
[0063] DSP59 is based on the code for playback transmitted from the flash memory 61, and is CRC (Cyclic Redundancy Check) about contents. After carrying out error detection by the method, it reproduces and the reproduced data (D1 shows in drawing 3) are supplied to the digital to analog circuit 63.
[0064] DSP59 supplies the clock LRCLK of operation which becomes the predetermined bit clock BCLK and the predetermined list of a frequency which were generated based on the master clock MCLK and the master clock MCLK in the internal oscillator circuit from the L channel clock LCLK of a frame unit, and the R channel clock RCLK to the digital-to-analog conversion circuit 63 while reproducing contents based on the master clock MCLK from dispatch child 59A which changes with Xtal by which was constituted by one and external was carried out to it with the dispatch circuit established in the interior.
[0065] When supplying an above-mentioned clock of operation to the digital-to-analog conversion circuit 63 according to the code for playback when reproducing contents, and not reproducing contents, DSP59 suspends supply of a clock of operation according to the code for playback, stops the digital-to-analog conversion circuit 63, and reduces the consumed electric power of the portable device 6 whole.
[0066] Similarly, external [of radiator 53A or 57A which CPU53 and the USB controller 57 also become with Xtal] is carried out, respectively, and it performs predetermined processing based on the master clock MCLK supplied from radiator 53A or 57A, respectively.
[0067] Thus, with constituting, the clock generation module for performing clock supply to each circuit block of CPU53, DSP59, and USB controller 57 grade becomes unnecessary, and the portable device 6 can be miniaturized while simplifying circuitry.
[0068] The digital-to-analog conversion circuit 63 changes the reproduced contents into the sound signal of an analog, and supplies this to an amplifying circuit 64. An amplifying circuit 64 amplifies a sound signal and supplies a sound signal to headphone through the headphone jack 65.
[0069] Thus, the portable device 6 suspends playback of contents, when press actuation of playback/the earth switch is carried out during playback, while reproducing the contents memorized by the flash memory 61 based on control of CPU53, when press actuation of playback/the earth switch is carried out.

[0070] The portable device 6 resumes playback of contents from the location stopped based on control of CPU53, when press actuation of playback/the earth switch is again carried out after a halt. When it passes for several seconds, without playback/earth switch suspending playback by press actuation, and adding actuation, the portable device 6 turns off a power source automatically, and reduces power consumption.
[0071] Incidentally, when press actuation of playback/the earth switch is carried out after the power source became off, the portable device 6 does not reproduce contents from the location which last time stopped, but reproduces them from the 1st music.
[0072] moreover, CPU53 of the portable device 6 -- the LCD controller 68 -- controlling -- a display 67 -- the condition of a playback mode, equalizer adjustments (for example, repeat playback, intro playback, etc.) (namely, adjustment of the gain corresponding to the frequency band of a sound signal), a tune number number, performance time amount, playback, a halt, and a rapid traverse -- information, such as conditions, such as return, sound volume, and a residue of a dry cell 51, is already displayed.
[0073] Furthermore, the portable device 6 stores the so-called FAT (File Allocation Table), such as a block location of a flash memory 61 where the number of the contents currently written in the flash memory 80 and each contents are written in EEPROM68, and various memory are recording information in addition to this.
[0074] Incidentally, in the gestalt of this operation, contents are treated considering 64KByte as 1 block, and the block location corresponding to the contents of one music is stored in FAT.
[0075] If the block location corresponding to the contents of the 1st music will be written in a flash memory 61 as FAT if the contents of the 1st music are written in a flash memory 61 by control of CPU53, next the contents of the 2nd music are written in a flash memory 61 when FAT is stored in a flash memory 61 for example, the block location corresponding to the contents of the 2nd music will be written in a flash memory 61 (the same field as the 1st music) as FAT.
[0076] Thus, FAT is rewritten at every writing of the contents to a flash memory 61, and the same data are further written in reserve at a duplex for protection of data.
[0077] If FAT is written in a flash memory 61, since the same field of a flash memory 61 will be rewritten twice corresponding to one writing of contents, by the count of little writing of contents, the count of rewriting specified to the flash memory 61 will be become, and rewriting of a flash memory 61 will become impossible.
[0078] Then, the portable device 6 makes EEPROM68 memorize FAT, and lessens the frequency of rewriting of the flash memory 61 corresponding to one writing of contents.
[0079] By making EEPROM68 memorize FAT with many counts of rewriting, the portable device 6 can increase the count which can do the writing of contents to dozens or more times as compared with the case where a flash memory 61 is made to memorize FAT. Furthermore, since CPU53 is made to write in so that FAT may be added to EEPROM68, it prevents lessening the frequency of rewriting of the same field of EEPROM68, and EEPROM68 rewriting for a short period of time, and becoming impossible.
[0080] The portable device 6 recognizes that USB connection was made based on the interrupt signal supplied to CPU53 from the USB controller 57, when it connects with a personal computer 1 through the USB cable 7 (this is hereafter called USB connection).

[0081] The portable device 6 controls a power circuit 52, and stops supply of the power from a dry cell 51 while it will receive supply of the external power of a convention current value from a personal computer 1 through the USB cable 7, if it recognizes that USB connection was made.
[0082] CPU53 stops processing of playback of the contents of DSP59, when USB connection is made. Thereby, CPU53 prevents that the external power supplied from a personal computer 1 exceeds a convention current value, and controls it to be always able to receive the external power of a convention current value.
[0083] Thus, if USB connection is made, since CPU53 will be switched to the power supplied from a personal computer 1 from the power supplied from a dry cell 51, the external power from the personal computer 1 with a cheap power unit price is used, the power consumption of the dry cell 51 with a high power unit price is reduced, and it can prolong the life of a dry cell 51 in this way.
[0084] In addition, when supply of external power is received from a personal computer 1 through the USB cable 7, by stopping regeneration of DSP59, CPU53 reduces the radiation from DSP59, and reduces much more radiation of the whole system which contains a personal computer 1 as the result.
[0085] The function of the personal computer 1 realized next by the program execution installed in the personal computer 1 is explained.
[0086] Drawing 4 is drawing which is realized by predetermined program execution etc. and in which showing the configuration of the function of a personal computer 1.
[0087] The contents manager 111 consists of two or more programs, such as the EMD selection program 131, check-in/check-out manager 132, the copy manager 133, the migration manager 134, the cipher system conversion program 135, the compression method conversion program 136, the encryption program 137, the use condition conversion program 139, the use condition manager 140, the authentication program 141, the decode program 142, the driver 143 for PD, the program 144 for purchase, and the program 145 for purchase.
[0088] the contents manager 111 -- for example, it is described by the instruction currently shuffled or the instruction enciphered, the contents of processing are concealed from the outside, and reading comprehension of the contents of processing becomes difficult (for example, a user cannot specify an instruction, even if it reads the contents manager 111 directly) -- it is constituted like.
[0089] When the contents manager 111 is installed in a personal computer 1, the EMD selection program 131 is not included in the contents manager 111, but is received from the EMD registration server 3 through a network 2 in the case of registration of EMD. The EMD selection program 131 chooses connection with that [EMD server 4 (4-1, 4-2, 4-3)], and makes the application 115 for purchase, or the program 144,145 for purchase perform the communication links (for example, download of contents when purchasing contents etc.) with the EMD server 4 (4-1, 4-2, 4-3).
[0090] Check-in/check-out manager 132 checks in at the contents which check out the contents stored in the contents file 161-1 - 161-N to the portable device 6 based on check-in or a setup of check-out and the use condition file 162-1 currently recorded on the contents database 114 - 162-N, or are memorized by the portable device 6.

[0091] Check-in/check-out manager 132 updates the use condition information stored in the use condition file 162-1 currently recorded on the contents database 114 - 162-N corresponding to processing of check-in or check-out.
[0092] The copy manager 133 copies the contents stored in the contents file 161-1 - 161-N to the portable device 6 based on the use condition file 162-1 currently recorded on the contents database 114 - 162-N, or copies contents to the contents database 114 from the portable device 6.
[0093] The migration manager 134 moves the contents stored in the contents file 161-1 - 161-N to the portable device 6 based on the use condition file 162-1 currently recorded on the contents database 114 - 162-N, or moves contents to the contents database 114 from the portable device 6.
[0094] The cipher system conversion program 135 is changed into the method of the same encryption as the contents stored in the contents file 161-1 on which the contents database 114 is recording the method of encryption of the contents which the application program 115 for purchase received from the EMD server 4-1, and the method of encryption of the contents which the program 144 for purchase received from the EMD server 4-2 - 161-N through a network 2.
[0095] The compression method conversion program 136 is changed into the method of the same compression as the contents stored in the contents file 161-1 on which the contents database 114 is recording the method of compression of the contents which the application program 115 for purchase received from the EMD server 4-1, and the method of compression of the contents which the program 144 for purchase received from the EMD server 4-2 - 161-N through a network 2.
[0096] It is read in CD and the encryption program 137 is enciphered by the method of the same encryption as the contents stored in the contents file 161-1 on which the contents database 114 is recording the contents (not enciphered) supplied from the sound recording program 113 - 161-N.
[0097] It is read in CD and compression/elongation program 138 is encoded by the method of the same coding as the contents stored in the contents file 161-1 on which the contents database 114 is recording the contents (not compressed) supplied from the sound recording program 113 - 161-N. Compression/elongation program 138 elongates the contents encoded (decode).
[0098] The use condition conversion program 139 is changed into the same format as the use condition information stored in the use condition file 162-1 on which the contents database 114 is recording the use condition information on the contents which the application program 115 for purchase received from the EMD server 4-1 (the so-called Usage Rule), and the use condition information on the contents which the program 144 for purchase received from the EMD server 4-2 - 162-N through a network 2.
[0099] The use condition manager 140 detects the alteration of use condition information based on the hash value corresponding to the use condition information stored in the use condition file 162-1 currently recorded on the contents database 114 - 162-N, before performing processing of the copy of contents, migration, check-in, or check-out. The use condition manager 140 updates the hash value corresponding to use condition information for the use condition information stored in the use condition file 162-1 currently recorded on the contents database 114 - 162-N accompanying

processing of the copy of contents, migration, check-in, or check-out corresponding to updating.

[0100] The authentication program 141 performs processing of the mutual recognition of the contents manager 111 and the application program 115 for purchase, and processing of the mutual recognition of the contents manager 111 and the program 144 for purchase. Moreover, the authentication program 141 has memorized the authentication key used by processing of the mutual recognition of the EMD server 4-3 and the program 145 for purchase.

[0101] The authentication key which the authentication program 141 uses by processing of mutual recognition is not memorized by the authentication program 141 when the contents manager 111 is installed in a personal computer 1, but when processing of registration is normally performed by the display operator guidance program 112, is supplied from the EMD registration server 3, and is memorized by the authentication program 141.

[0102] The decode program 142 decodes contents, when a personal computer 1 reproduces the contents stored in the contents file 161-1 which the contents database 114 is recording - 161-N.

[0103] The driver 143 for PD supplies the command which makes the portable device 6 perform predetermined processing to contents or the portable device 6, when you check out predetermined contents to the portable device 6, or when you check in at predetermined contents from a portable device.

[0104] The program 144 for purchase is installed with the contents manager 111, is supplied through a network 2 from the EMD registration server 3, or is recorded on predetermined CD and supplied. The program 144 for purchase transmits and receives the contents manager 111 and data through the interface of the predetermined format which the contents manager 111 has, when installed in a personal computer 1.

[0105] the program 144 for purchase -- for example, it is described by the instruction currently shuffled or the instruction enciphered, the contents of processing are concealed from the outside, and reading comprehension of the contents of processing becomes difficult (for example, a user cannot specify an instruction, even if it reads the program 144 for purchase directly) -- it is constituted like.

[0106] The program 144 for purchase receives contents from the EMD server 4-2 while requiring transmission of predetermined contents of the EMD server 4-2 through a network 2. Moreover, the program 144 for purchase performs processing of accounting, when receiving contents from the EMD server 4-2.

[0107] The program 145 for purchase is a program installed with the contents manager 111, and it receives contents from the EMD server 4-3 while it requires transmission of predetermined contents of the EMD server 4-3 through a network 2. Moreover, the program 145 for purchase performs processing of accounting, when receiving contents from the EMD server 4-3.

[0108] The display operator guidance program 112 displays the image of a predetermined window on a display 20 based on the filtering data file 181, the display data file 182, an image file 183-1 - 183-K, or the hysteresis data file 184, and directs activation of processings, such as check-in or check-out, based on the actuation to a keyboard 18 or a mouse 19 at the contents manager 111.

[0109] The filtering data file 181 stores the data for making weighting each contents stored in the contents file 161-1 currently recorded on the contents database 114 - 161-N, and is recorded on HDD21.
[0110] The display data file 182 stores the data corresponding to the contents stored in the contents file 161-1 currently recorded on the contents database 114 - 161-N, and is recorded on HDD21.
[0111] An image file 183-1 - 183-K store the image corresponding to the contents file 161-1 currently recorded on the contents database 114 - 161-N, or the image corresponding to the package mentioned later, and are recorded on HDD21.
[0112] Hereafter, when it is not necessary to distinguish an image file 183-1 - 183-K separately, an image file 183 is only called.
[0113] The contents stored in the contents file 161-1 currently recorded on the contents database 114 - 161-N store historical data, such as a checked-out count, a count at which he checked in, and its date, and the hysteresis data file 184 is recorded on HDD21.
[0114] The display operator guidance program 112 receives the key for authentication, and the EMD selection program 131 from the EMD registration server 3, and supplies the key for authentication, and the EMD selection program 131 to the contents manager 111 while it transmits ID of the contents manager 111 beforehand memorized to the EMD registration server 3 through a network 2 at the time of processing of registration.
[0115] The sound recording program 113 displays the image of a predetermined window, and reads data, such as sound recording time amount of contents, from CD which is the optical disk 42 with which the drive 22 was equipped based on the actuation to a keyboard 18 or a mouse 19.
[0116] The sound recording program 113 minds a network 2 based on the sound recording time amount of the contents currently recorded on CD etc. While requiring transmission of the data (for example, music name etc.) corresponding to the contents currently recorded on the WWW server 5-1 or 5-2 by the data (for example, an album name or an artist name etc.) or CD corresponding to CD The data corresponding to the contents currently recorded on the data or CD corresponding to CD from the WWW server 5-1 or 5-2 are received.
[0117] The sound recording program 113 supplies the data corresponding to the contents currently recorded on the data or CD corresponding to received CD to the display operator guidance program 112.
[0118] Moreover, when directions of sound recording are inputted, the sound recording program 113 reads contents from CD which is the optical disk 42 with which the drive 22 was equipped, and outputs them to the contents manager 111.
[0119] The contents which the contents database 114 is compressed by the predetermined method supplied from the contents manager 111, and are enciphered by the predetermined method are stored in either the contents file 161-1 - 161-N (it records on HDD21). The contents database 114 is stored in either the use condition file 162-1 corresponding to the contents file 161-1 by which the use condition information corresponding to the contents stored in the contents file 161-1 - 161-N, respectively is stored in contents - 161-N - 162-N, respectively (it records on HDD21).
[0120] The contents database 114 may record the contents file 161-1 - 161-N, or the use condition file 162-1 - 162-N as a record.

[0121] For example, the use condition information corresponding to the contents stored in the contents file 161-1 is stored in the use condition file 162-1. The use condition information corresponding to the contents stored in contents file 161-N is stored in use condition file 162-N.
[0122] Hereafter, when it is not necessary to distinguish the contents file 161-1 - 161-N separately, the contents file 161 is only called. Hereafter, when it is not necessary to distinguish the use condition file 162-1 - 162-N separately, the use condition file 162 is only called.
[0123] The application program 115 for purchase is supplied through a network 2 from the EMD registration server 3, or is recorded and supplied to predetermined CD-ROM. The application program 115 for purchase receives contents from the EMD server 4-1, and supplies them to the contents manager 111 while it requires transmission of predetermined contents of the EMD server 4-1 through a network 2. Moreover, the application program 115 for purchase performs processing of accounting, when receiving contents from the EMD server 4-1.
[0124] Next, matching with the data stored in the display data file 182, and the contents file 161-1 stored in the contents database - 161-N is explained.
[0125] The contents stored in either the contents file 161-1 - 161-N belong to a predetermined package. A package is either an original package and my selection package or a filtering package more at a detail.
[0126] One or more contents belong and an original package is equivalent to the classification (for example, it corresponds to the so-called album) of the contents in the EMD server 4, or CD of one sheet. Contents cannot belong to one of original packages, and cannot belong to two or more original packages. Moreover, the original package with which contents belong cannot be changed. A user can edit a part of information corresponding to an original package (modification of the information which information added or added).
[0127] One or more contents from which the user chose the my selection package as arbitration belong. A user can edit into arbitration whether which contents belong to a my selection package. Contents can belong to one or more my selection packages at coincidence. Moreover, contents do not need to belong to which my selection package.
[0128] The contents chosen based on the filtering data stored in the filtering data file 181 belong to a filtering package. Filtering data are supplied through a network 2 from the EMD server 4 or the WWW server 5, or are recorded on predetermined CD and supplied. A user can edit the filtering data stored in the filtering data file 181.
[0129] Filtering data serve as criteria which choose predetermined contents or compute the weight corresponding to contents. For example, if the filtering data corresponding to the J-POP (pop of Japan) top ten of this week are used, a personal computer 1 can specify the contents of the 10th place of the pop of Japan of the contents of the 1st place of the pop of Japan of this week - this week.
[0130] The filtering data file 181 contains the filtering data with which the period checked out in January [past] chooses contents as long order, the filtering data which choose contents with many counts checked out at past half a year, or the filtering data which chooses the contents by which the alphabetic character of "love" is contained in the music name.

[0131] Thus, the contents of a filtering package make the indicative data 221 (the data which the user set as the indicative data 221 for contents are included) for contents corresponding to contents or historical data 184, and filtering data correspond, and are chosen.
[0132] A driver 117 outputs the analog signal corresponding to the contents which drove the voice-input/output interface 24 on the radical of control, such as the contents manager 111, and outputted to it the contents which inputted the contents which are digital data supplied from the outside, and supplied the contents manager 111, or were supplied from the contents database 114 through the contents manager 111 as digital data, or were supplied to it from the contents database 114 through the contents manager 111.
[0133] Drawing 5 is drawing showing the example of the display operator guidance window which the operator guidance program 112 displays on a display 20, when starting the display operator guidance program 112.
[0134] In order to edit the carbon button 203 for displaying the field which sets up processing of the carbon button 202 for making a display operator guidance window start the carbon button 201 for starting the sound recording program 113, and the EMD selection program 131, check-in, or check-out, and a my selection package, the carbon button 204 grade for displaying the field is arranged.
[0135] When the carbon button 205 is chosen, the data corresponding to an original package are displayed on the field 211. When the carbon button 206 is chosen, the data corresponding to a my selection package are displayed on the field 211. When the carbon button 207 is chosen, the data corresponding to a filtering package are displayed on the field 211.
[0136] The data displayed on the field 211 are data about a package, for example, are a package name or an artist name.
[0137] for example, -- drawing 5 -- setting -- a package -- a name -- " -- the first -- " -- and -- an artist -- a name -- " -- A -- Taro -- " -- a package -- a name -- " -- second -- " -- and -- an artist -- a name -- " -- A -- Taro -- " -- etc. -- the field -- 211 -- displaying -- having .
[0138] The data corresponding to the contents belonging to the package chosen in the field 211 are displayed on the field 212. The data displayed on the field 212 are for example, a music name, performance time amount, or the count that can be checked out.
[0139] For example, in drawing 5 , since the package corresponding to package name" second" is chosen Bar" and the count which can be checked out of package name "music name corresponding to contents belonging to package corresponding to second"" south (for example, one of the eighth notes is equivalent to one check-out, and an eighth note shows two check-out by two), and a list -- a music name -- "a north graveyard", the count (an eighth note shows one check-out by one) which can be checked out are displayed on the field 212.
[0140] Thus, it is shown that corresponding contents can check out once one eighth note as a count which is displayed on the field 212 and which can be checked out.
[0141] The rest as a count which is displayed on the field 212 and which can be checked out cannot check out corresponding contents (the count which can be checked out is 0.). (-- however, a personal computer 1 can reproduce the contents.) -- things are

shown. Moreover, the G clef as a count which is displayed on the field 212 and which can be checked out shows what no limit is in the count of check-out of corresponding contents (he can check out any number of times).
[0142] In addition, as shown in drawing 5 , it not only displays the count which can be checked out by the number of predetermined graphic forms (for example, a circle, a star, the moon, etc. are sufficient), but you may display it in a figure etc.
[0143] Moreover, the field 208 which displays the image matched with the package or contents chosen on a display operator guidance window (it corresponds to either the image file 183-1 of drawing 4 - 183-K) is arranged. A carbon button 209 is clicked when reproducing the contents chosen (the voice corresponding to contents is made to output to a loudspeaker 45).
[0144] When a carbon button 205 is chosen and the data corresponding to an original package are displayed on the field 211, and choosing the music name of the predetermined contents currently displayed on the field 212 and operating elimination, the display operator guidance program 112 makes the predetermined contents stored in the contents database 114 corresponding to the music name chosen as the contents manager 111 eliminate.
[0145] When the carbon button (carbon button 255 mentioned later) of the window which the sound recording program 113 displays is chosen, it is (activated) and the contents read from CD are recorded on the contents database 114, the display operator guidance program 112 displays the field 213 which displays the music name of the contents memorized by the portable device 6 beforehand specified as the display operator guidance window.
[0146] When the carbon button of the window which the sound recording program 113 displays is chosen and the contents read from CD are recorded on the contents database 114, the display operator guidance program 112 makes the portable device 6 specified beforehand check out the contents which were recorded on the contents database 114 at the contents manager 111 and which were read from CD.
[0147] The music name of contents is made to correspond to the field 213, and the notation which shows whether the contents can check in at a personal computer 1 is displayed on the leftmost of the field 213. For example, "O" located in the leftmost of the field 213 shows what (that is, the personal computer 1 was checked out) the contents corresponding to the music name of contents can check in at a personal computer 1. "x" located in the leftmost of the field 213 shows what (that is, a personal computer 1 is not checked out, for example, other personal computers were checked out) the contents corresponding to the music name of contents cannot check in at a personal computer 1.
[0148] When a display operator-guidance program 112 displays the field 213 on a display operator-guidance window, a display operator-guidance program 112 displays the carbon button 215 which performs the carbon button 210 and the check-in, or the check-out for closing the field 214 and the field 213 which display the name of the portable package (par cage with which the contents memorized by the portable device 6 belong) with which the contents memorized by the portable device 6 beforehand specified as the display operator-guidance window belong.
[0149] When the display operator guidance program 112 displays the field 213 on a display operator guidance window, furthermore, the display operator guidance program 112 In a display operator guidance window The carbon button 216 which sets up check-

out of the contents corresponding to the music name chosen in the field 212, A setup of the carbon button 217 which sets up check-in of the contents corresponding to the music name chosen in the field 213, the carbon button 218 which sets up check-in of all the contents corresponding to the contents name displayed on the field 213 and check-in, or check-out The carbon button 219 to cancel is arranged.
[0150] Only by setup of a carbon button 216 thru/or the check-in by actuation of 219, or check-out, a personal computer 1 does not perform processing of check-in or check-out.
[0151] When a carbon button 215 is clicked after carrying out a setup of a carbon button 216 thru/or the check-in by actuation of 219, or check-out, the display operator guidance program 112 makes the contents manager 111 perform processing of check-in or check-out. When a carbon button 215 is clicked, namely, the display operator guidance program 112 It is based on a setup of check-in or check-out. To the contents manager 111 While making contents transmit to the portable device 6 or making the predetermined commands (for example, command which makes the predetermined contents which the portable device 6 has memorized eliminate) corresponding to check-in transmit The use condition information stored in the use condition file 162 corresponding to the transmitted contents or the command is made to update.
[0152] When check-in or check-out is performed, the display operator guidance program 112 updates the historical data stored in the hysteresis data file 184 corresponding to the contents which transmitted, or the transmitted command. Historical data consist of the name of the information which specifies the contents checked in or checked out or the date checked in or checked out in the contents, and the portable device 6 with which he was checked out in the contents etc.
[0153] Since processing of a setup of check-in or check-out can be performed in a short time, a user can know quickly the condition after check-in or activation of processing of check-out, the count of processing of the check-in which time amount requires, or check-out can be reduced, and the whole (a setup and activation are contained) time amount required for check-in or check-out can be shortened.
[0154] Drawing 6 is drawing explaining the example of the window which the sound recording program 113 displays on a display 20.
[0155] For example, the sound recording program 113 displays the title of CDs, such as "ASHINKURONAIZUDO", on the field 251 based on the information on CD received from the WWW server 5-2. Based on the information on CD received from the WWW server 5-2, the sound recording program 113 displays artist names, such as an "arrowhead", on the field 252.
[0156] Based on the information on CD received from the WWW server 5-2, the sound recording program 113 displays music names, such as "heat", a "planet", "black", and "Seoul", on the part which displays the music name of the field 253. Similarly, the sound recording program 113 displays artist names, such as an "arrowhead", on the part which displays the artist of the field 253.
[0157] After the sound recording program 113 receives the information on predetermined CD, the sound recording program 113 stores the information on CD in the predetermined directory of HDD21.
[0158] When a carbon button 254 etc. is clicked and directions of acquisition of the information on CD are received, as for the sound recording program 113, the predetermined directory of HDD21 is searched first. The sound recording program 113

makes it choose whether the dialog box which is not illustrated is displayed and the information on CD stored in the user to the directory is used, when the information on CD is stored in the directory.
[0159] When the carbon button 256 which directs initiation of the sound recording of the contents arranged in the window which the sound recording program 113 displays is clicked, the sound recording program 113 supplies the contents which read contents from CD stored in the drive 22, and were read from CD to the contents manager 111 with the information on CD. Compressing compression/elongation program 138 of the contents manager 111 by the method of predetermined compression of the contents supplied from the sound recording program 113, the encryption program 137 enciphers the compressed contents. Moreover, the use condition conversion program 139 is compressed and generates the use condition information corresponding to the enciphered contents.
[0160] The contents manager 111 is compressed and supplies the enciphered contents to the contents database 114 with use condition information.
[0161] The contents database 114 stores use condition information in the use condition file 162 while it generates the contents file 161 and the use condition file 162 corresponding to the contents which received from the contents manager 111 and stores contents in the contents file 161.
[0162] The contents manager 111 supplies the information and use condition information on CD which were received from the sound recording program 113 to the display operator guidance program 112, when the use condition information corresponding to contents and contents is stored in the contents database 114.
[0163] The display operator guidance program 112 generates the data for a display stored in the display data file 182 based on the use condition information corresponding to the contents stored in the contents database 114 by processing of sound recording, and the information on CD.
[0164] In the window which the sound recording program 113 displays, when the contents read from CD are further recorded on the contents database 114, the carbon button 255 which sets up whether the portable device 6 is made to check out the contents read from CD is arranged automatically.
[0165] For example, when a carbon button 255 is clicked, the sound recording program 113 displays the pull down menu which shows the portable device 6. When a user chooses the portable device 6 from the pull down menu, he checks out the contents automatically recorded on the selected portable device 6 from CD. When a user chooses "he not checking out" out from the pull down menu, when contents are recorded from CD, he does not check out a personal computer 1.
[0166] Thus, when the contents read from CD are recorded on the contents database 114 only by activating the carbon button 255 of the window which the sound recording program 113 displays, the contents read from CD to the portable device 6 specified beforehand can be made to check out a personal computer 1.
[0167] (2) the contents distribution contractor who is at the handling during a different format, and the time, and offers a music content -- many -- existing -- every distribution contractor -- the cipher system and compression method of the contents -- formats of use condition information differ further. Therefore, generally the user had to purchase the contents management application and the portable device for playback, or check-

in/check-out for every distribution contractor of contents to receive offer. Therefore, the user was able to deal with the music content stored on one personal computer neither with one management application nor portable device.
[0168] So, in this system, the contents from which a format differs for every distribution contractor in this way are systematically dealt with on the personal computer 1.
[0169] Hereafter, the unific handling of the contents from which a format differs for every distribution contractor in this music content distribution system is explained with reference to drawing 7 .
[0170] Two or more EMD servers connected to the network 2 shall be EMD (server A) 4-1 which distributes the music content offered from the music offer firm A, EMD (server B) 4-2 which distribute the music content offered from the music offer firm B, and EMD (server X) 4-3 which distributes the music content offered from the music offer firm X. Each EMD server 4 (4-1, 4-2, 4-3) provides for the personal computer 1 in which a user has the music content to which lineup was carried out original with each company through a network 2. Moreover, in each EMD server 4 (4-1, 4-2, 4-3), the music content is distributed with a method which the method of each company with original cipher system of a music content, format of use condition (Usage Rule) information, compression method of a music content, charging system of a music content, etc. is adopted, and is different, respectively.
[0171] In a personal computer 1, as application software for performing playback, management, etc. of a music content the application for playback (A) which performs purchase and management of a music content, and playback from EMD (server A) 4-1 -- 311 -- the application for playback (B) which performs purchase and management of a music content, and playback from EMD (server B) 4-2 -- 312 -- a music content -- portable -- a device -- (-- A --) -- six - one -- transmitting -- a device driver -- (-- A --) -- 313 -- a music content -- portable -- a device -- (-- B --) -- six - two -- transmitting -- a device driver -- (-- B --) -- 314 -- installing -- having -- **** . In addition, the application 311,312 for playback shown by this drawing 7 corresponds to the application program 115 for purchase and driver 117 which were shown by drawing 4 .
[0172] Moreover, the comprehension management unit (X) 315 which performs comprehensive management of all the music contents stored in HDD21 is installed in the personal computer 1. This comprehension management unit (X) 315 is further constituted by the reception interface 316 for EMD, the transmitting interface 317 for EMD, and the driver 318 for PD.
[0173] moreover, portable here -- (Device A) 6-1 is equipment of the dedication corresponding to the music offer firm A, and it is portable -- (Device B) 6-2 are equipment of the dedication corresponding to the music offer firm B, and they are portable -- (Device X) 6-3 shall be equipment of the dedication corresponding to the music offer firm X In addition, the music content stored in the memory card is enciphered with the original cipher system of each music offer firm, and formats of the compression method or use condition information also differ here. Therefore, direct continuation shall be carried out, for example to other device drivers etc., and a music content shall be transmitted no longer.
[0174] The application 311 for playback (A) performs processing which downloads the processing which uploads connection processing with an EMD server, a log file, etc., a music content, a contents key, use condition information, etc. This application 311 for

playback (A) performs connection processing only to a corresponding EMD server. Here, the application 311 for playback (A) cannot perform processing corresponding to EMD (server A) 4-1, and cannot perform connection processing to other EMD servers. moreover, the application 311 for playback (A) processing [authentication] and is [at the time of connecting with EMD (server A) 4-1] portable -- encryption/decryption processing of the music content stored in the authentication processing at the time of connecting with (Device A) 6-1 and HDD21 and use condition information etc. is performed. The application 311 for playback (A) enciphers the music content downloaded from EMD (server A) 4-1, and its use condition information with a contents key, enciphers this contents key with a session key, and stores it in HDD21. In addition, the respectively original method is used for the method of encryption processing with each application for playback. Therefore, if it is not the application for playback of dedication even if it is the music content stored in same HDD21 in a personal computer 1, a code can be decoded no longer in other applications for playback.

[0175] Moreover, the application 311 for playback (A) also performs management of the use condition information added to each music content. For example, the application 311 for playback (A) processes carrying out 1 batch decrement of the count limit value of playback or a duplicate, whenever it performs playback and reproduction, when the count limit value of playback is described by use condition information and the limit of the count of playback of contents is carried out etc.

[0176] Moreover, the application 311 for playback (A) transmits the music content and use condition information which self has managed on HDD21 to the reception interface 316 for EMD of the comprehension management unit (X) 315.

[0177] The application 312 for playback (B) performs processing which downloads the processing which uploads connection processing with an EMD server, a log file, etc., a music content, a contents key, use condition information, etc. This application 312 for playback (B) performs connection processing only to a corresponding EMD server. The application 312 for playback (B) cannot perform processing corresponding to EMD (server B) 4-2, and, specifically, cannot perform connection processing to other EMD servers. moreover, the application 312 for playback (B) processing [authentication] and is [at the time of connecting with EMD (server B) 4-2] portable -- encryption/decryption processing of the music content stored in the authentication processing at the time of connecting with (Device B) 6-2 and HDD21 and use condition information etc. is performed. The application 312 for playback (B) enciphers the music content downloaded from EMD (server B) 4-2, and its use condition information with a contents key, enciphers this contents key with a session key, and stores it in HDD21.

[0178] Moreover, the application 312 for playback (B) also performs management of the use condition information added to each music content. For example, the application 312 for playback (B) processes carrying out 1 batch decrement of the count limit value of playback or a duplicate, whenever it performs playback and reproduction, when the count limit value of playback is described by use condition information and the limit of the count of playback of contents is carried out etc.

[0179] Moreover, the application 312 for playback (B) transmits the music content and use condition information which self has managed on HDD21 to the reception interface 316 for EMD of the comprehension management unit (X) 315.

[0180] a device driver (A) 313 is portable -- it is the application software which performs a transfer of the music content of (Device A) 6-1 etc. a device driver (A) 313 is portable -- a music content is transmitted to (Device A) 6-1.
[0181] a device driver (B) 314 is portable -- it is the application software which performs a transfer of the music content of (Device B) 6-2 etc. a device driver (B) 314 is portable -- a music content is transmitted to (Device B) 6-2.
[0182] comprehension -- management -- a unit -- (-- X --) -- 315 -- EMD -- a server -- (-- X --) -- four - three -- from -- a music content -- offer -- winning popularity -- music -- offer -- a firm -- X -- dedication -- application software -- it is -- while -- a device driver -- (-- A --) -- 313 -- and -- a device driver -- (-- B --) -- 314 -- playback -- ** -- application -- (-- A --) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- between -- a music content -- and -- use -- conditions -- information -- a transfer -- carrying out -- a personal computer -- one -- inside -- a music content -- comprehensive -- management -- carrying out -- management -- software -- it is also . moreover, the dedication which is the music regenerative apparatus of a pocket mold about the music content to which self manages is portable -- it can transmit to (Device X) 6-3.
[0183] In addition, this comprehension management unit (X) 115 performs processing corresponding to the contents manager 111 shown in drawing 4 . [0184] the interface module for connection with (Device X) 6-3 with the portable driver 318 for PD -- it is -- this -- portable -- the authentication processing and encryption processing between (Device X) 6-3 are performed. moreover -- PD -- ** -- a driver -- 318 -- others -- portable -- a device -- eight -- nine -- a music content -- etc. -- transmitting -- a case -- **** -- a device driver -- (-- A --) -- 313 -- a device driver -- (-- B --) -- 314 -- minding -- a music content and use condition information -- transmitting .
[0185] EMD -- ** -- reception -- an interface -- 316 -- playback -- ** -- application -- (-- A --) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- from -- a music content -- and -- use -- conditions -- information -- reception -- EMD -- a server -- (-- X --) -- four - three -- from -- a network -- two -- minding -- transmitting -- having had -- a music content -- and -- use -- conditions -- information -- reception -- and -- PD -- ** -- a driver -- 318 -- between -- a music content -- and -- use -- conditions -- information -- transmission and reception -- carrying out .
[0186] EMD -- ** -- reception -- an interface -- 316 -- playback -- ** -- application -- (-- A --) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- from -- a music content -- and -- use -- conditions -- information -- receiving -- a case -- **** -- mutual recognition -- processing -- a cipher system -- conversion -- transmitting -- a music content -- adding -- having had -- use -- conditions -- information -- a format -- conversion -- transmitting -- a music content -- compression -- a method -- conversion -- etc. -- carrying out . a cipher system -- use -- conditions -- information -- compression -- a method -- conversion -- playback -- ** -- application -- (-- A --) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- using -- **** -- a method -- from -- comprehension -- management -- a unit -- (-- X --) -- 315 -- using -- **** -- a method -- changing -- having . The method which the comprehension management unit (X) 315 uses here is hereafter called a unification transfer protocol. and -- EMD -- ** -- reception -- an interface -- 316 -- such -- unification -- a transfer protocol -- having changed -- a music content -- and -- use -- conditions -- information -- PD -- ** -- a driver -- 318 -- minding -- a device driver -- (-- A --) -- 313 -- a device driver -- (-- B --) -- 314 -- transmitting . moreover, the reception

interface 316 for EMD is portable through the driver 318 for PD in the music content and use condition information which were changed into the unification transfer protocol -- it transmits to (Device X) 6-3.
[0187] thus -- EMD -- a server -- (-- A --) -- four - one -- and -- EMD -- a server -- (-- B --) -- four - two -- from -- providing -- having -- a music content -- once -- playback -- ** -- application -- (-- A --) -- 311 -- and -- playback -- ** -- application -- (-- B --) -- 312 -- downloading -- having -- a music content -- a cipher system -- compression -- a method -- use -- conditions -- information -- unification -- a transfer protocol -- changing -- having -- comprehension -- management -- a unit -- (-- X --) -- 315 -- transmitting -- having . The comprehension management unit (X) 315 is manageable in generalization in the music content of EMD (server A) 4-1, an EMD server (B4 -2), and each contents offer firm that downloaded from EMD (server X) 4-3.
[0188] Moreover, the reception interface 316 for EMD has the function of the duplicate (copy) of a music content, migration (MUBU), check-in, and check-out.
[0189] EMD -- ** -- reception -- an interface -- 316 -- a user -- from -- a duplicate -- an instruction -- migration -- an instruction -- following -- for example, -- playback -- ** -- application -- (-- A --) -- 311 -- playback -- ** -- application -- (-- B --) -- 312 -- managing -- having -- **** -- a music content -- comprehension -- management -- a unit -- (-- X --) -- 315 -- a duplicate -- migration -- carrying out -- processing -- carrying out . In this case, the reception interface 316 for EMD changes a description format of the cipher system of a music content and a compression method, and use conditions, and let it be a unification transfer protocol.
[0190] Moreover, according to CD ripping instruction from a user, or a check-in instruction, processing which reproduces and checks in at the music content stored in external media and the portable devices 6 (6-1, 6-2, 6-3), such as a compact disk, at the comprehension management unit (X) 315 is performed. In this case, if the description format of the cipher system of a music content and a compression method, and use conditions is not made into the unification transfer protocol, the reception interface 316 for EMD performs these conversion, and let it be a unification transfer protocol.
[0191] moreover, portable in the music content managed by the comprehension management unit (X) 315 according to the check-out instruction from a user -- processing recorded on (Device X) 6-3 is performed. In this case, if the description format of the cipher system of a music content and a compression method, and use conditions is not made into the unification transfer protocol, the reception interface 316 for EMD performs these conversion, and let it be a unification transfer protocol. Moreover, 1 **** of the counts of use conditions which can be checked out is carried out in this case.
[0192] Moreover, in the comprehension management unit (X) 315, as shown in drawing 8 , a unification transfer protocol is formed in the lower layer of the application layer, and data transfer with other applications for playback is performed in this layer. And furthermore the comprehension management unit (X) 315 is this unification transfer protocol, it is performing data transmission and reception with EMD (server X) 4-3 by setting a lower layer to http (hiperText Transfer Protocol).
[0193] In the above music content distribution systems of a configuration, the comprehension management unit (X) 315 acquires the music content distributed from EMD (server A) 4-1 and EMD (server B) 4-2, and playback and management are

performed. and EMD (server X) 4-3 and the EMD server (A) 4 -- portable in the music content distributed from -1 and EMD (server B) 4-2 -- it can transmit now to (Device X) 6-3.
[0194] Thus, focusing on the comprehension management unit (X) 315, between each application for playback, and a device driver, conversion of the cipher system of the music content to transmit, conversion of a format of the use condition information added to the music content to transmit, and conversion of the compression method of the music content to transmit are performed, and a transfer of a music content is performed in a music content distribution system using a unification transfer protocol. therefore -- for example, the music content downloaded from EMD server B4 -2 with the application 312 for playback (B) in the music content list downloaded from EMD (server A) 4-1 with the application 311 for playback (A) can be transmitted to the comprehension management unit (X) 315. for this reason -- for example, portable in an artist's music content offered only from the music offer firm A -- it can transmit to (Device X) 6-3. namely, the music content of various methods stored in the hard disk of a personal computer 1 in this music content distribution system since the cipher system of a music content, a format of use condition information, the compression method of a music content, etc. are changed into a unification transfer protocol -- the comprehension management unit (X) 315 -- portable -- it is reproducible (Device X) 6-3. Especially, in a music content distribution system, the degree of freedom [music content / the] of handling can be enlarged, aiming at protection of the copyright of a music content, since a cipher system and use condition information are changed in the case of a transfer.
[0195] That is, in a music content distribution system, between the applications for playback which perform playback and control of a music content, conversion of a cipher system and use condition information is performed at least, and a transfer of a music content and use condition information is performed. By this, in a music content distribution system, even if two or more applications for playback exist, the music content stored in HDD21 in a personal computer 1 can be moved freely, and a unific music content can be managed. Moreover, since use condition information is also transmitted with a music content, use conditions do not overlap to one music content, and the copyright of a music content can also be protected certainly.
[0196] (3) use condition information (explanation of the use condition information that it is generally used), next, explain an example of a format of use condition information used for the application 311 for playback (A).
[0197] In the application 311 for playback (A), the use condition information described by the tabular format as shown in drawing 9 (a), for example is used.
[0198] In the left column of a table, the policy of use conditions is described in the direction of a train, and the concrete value of each policy is described by the right column. For example, the day (from) which can be playback started, a playback end date (to), the price (pay/play) to one playback, etc. are described as a policy. Such use condition information is in the condition added to each music content, as shown in drawing 9 (b), and it is distributed from EMD (server A) 4-1. The application 311 for playback (A) controls a music content according to the policy described and its value. For example, suppose that the prices [as opposed to / as opposed to / in the day (from) which can be playback started / use condition information / November 24, 99 and one playback in a playback end date (to)] (pay/play) are described to be yes / 10 yen on

October 25, 99. In this case, even if playback of that music content is enabled from October 25, 99 and there is a playback instruction from a user before it, it forbids playback. Moreover, if playback of the music content is enabled till November 24, 99 and it serves as it or later, it will eliminate the music content. Moreover, the music content keeps separately the count which it is set up so that 10 yen accounting may be performed at every one playback, for example, the user reproduced as log information, and performs accounting only for the count which viewed and listened to the log information to the user who uploaded, viewed and listened to EMD (server A) 4-1.
[0199] (Explanation of the use condition information that the comprehension management unit (X) 315 uses), below, the use condition information that the comprehension management unit (X) 315 uses is explained. The use condition information which gives explanation below is added to the music content downloaded from EMD (server X) 4-3, and in case the above-mentioned comprehension management unit (X) 315 controls the music content, it is used. moreover -- this -- use -- conditions -- information -- playback -- ** -- application -- (-- A --) -- 311 -- comprehension -- management -- a unit -- (-- X --) -- 315 -- between -- and -- playback -- ** -- application -- (-- B --) -- 312 -- comprehension -- management -- a unit -- (-- X --) -- 315 -- between -- a music content -- a transfer -- carrying out -- the time -- unification -- a format -- ****** -- using -- having . Hereafter, this use condition information is called unification use condition information.
[0200] Unification use condition information consists of an index file 331, an automaton file 332, a parameter file 333, and a history file 334, as shown in drawing 10 . Each file is described in XML (eXtensible Markup Language) language.
[0201] The reference source of each file etc. is described by the index file 331.
[0202] As shown in drawing 11 , the certificate of attestation (Cert) 344 for verifying the signature (Sig) 343 of the automaton description section 341 use conditions were described to be with the automaton, the authorization code (MAC:Message Authentication Code) 342 with a contents key, and a contents provider, and this signature is added to the automaton file 332. Here, a contents provider's private key and public key which created KC and contents for the contents key are set to K-1E and K1E, respectively.
[0203] The operating state of a music content is described by Extended State Machine the automaton description section 341 was described to be in the tuple train.
[0204] The set of the operating state of a current music content is set to Q, and, specifically, Q' is expressed with the automaton description section 341 for the set of the operating state of the music content after it sets the set of the input symbol showing the event of a music content to sigma and it carries out a state transition as follows.
Q'= {d|d=delta(q, alpha) |q Q, alpha sigma, and delta:Qxsigma->Q}
As shown in this formula, the set of condition Q' after carrying out a state transition is expressed as d. This d is defined by the function delta with Variables q and alpha. q shows one operating state in the set Q of the operating state of a music content. alpha shows one event in the set sigma of an event. And Function delta Q Reaches, is sigma Described, comes, and is the map to Q of a set.
[0205] and the above Q, sigma, and Q' -- being based -- every -- tuple -- {<q, alpha, d> |q, d Q, alpha sigma}

It expresses by carrying out. In addition, <q, alpha, d> show combination with the permutation of q, alpha, and d.
[0206] It reproduces and (Play) reproduces (copy), and pays to sigma here, and events, such as the amount of money (pay Y), time (from YMD) which can be playback started, playback termination time (to YMD), usable days (inch Ddays), and a null event (epsilon), are described as follows.
sigma= {Play, copy, pay Y, from YMD, to YMD, in Ddays, epsilon}
Thus, the automaton description section 341 is described as mentioned above.
[0207] The concrete example of description to this automaton description section 341 is explained.
[0208] For example, the example of description by the tuple train of the automaton in which transition of a music content as shown in drawing 12 of operation is shown is shown in drawing 13 .
[0209] This automaton carries out a state transition which is explained below.
[0210] First, it changes in a condition q1 and the condition q5 from an initial state q0. After a condition q1 and a condition q5, it operates in parallel, respectively.
[0211] If the predetermined amount of money (for example, 10 yen) pays and an event (pay10) occurs in the condition q1, it will change to a condition q2. In the condition q2, if a play event (play) occurs, it will change to a condition q1. That is, with this automaton, if payment of 10 yen is carried out, it is shown that playback of a music content is attained only once. Moreover, if the predetermined amount of money (for example, 1000 yen) pays and an event (a. pay1000) occurs in the condition q1, it will change to a condition q3. In the condition q3, if a play event (play) occurs, it will change in this condition q3 again. That is, with this automaton, if payment of 1000 yen is carried out, it is shown that a music content becomes a count reproducible without a limit. Moreover, if the n times as much amount of money as 1 time of the playback amount of money (for example, 10 yen) pays and an event (pay10xn) occurs in the condition q1, it will change to a condition q4. After changing to a condition q4, if a play event (play) occurs, it will change in this condition q4 again. And in this condition q4, if n times of play events occur, it will change in the condition q1. That is, with this automaton, if payment of 10xn yen is carried out, it is shown that playback of a music content is attained n times.
[0212] Moreover, if the predetermined amount of money (for example, 100 yen) pays and an event (pay100) occurs in the condition q5, it will change to a condition q6. In the condition q6, if a copy event (copy) occurs, it will change to a condition q5. Moreover, in the condition q6, if a copy event (copy) occurs, it will change to a condition q8. In the condition q8, if a play event (play) occurs, it will change in this condition q8 again. Moreover, in this condition q8, if a copy event (copy) occurs, it will change in the condition q9. It is in the termination condition that it changes to no condition and an event cannot be generated in the condition q9, either. That is, with this automaton, if payment of 100 yen is carried out, it is shown that a music content can be copied once to other devices. Moreover, with this automaton, although any number of times of reproducing the copied music content are possible, when it copies to other devices etc., it is shown that playback becomes impossible.
[0213] Moreover, if the predetermined amount of money (for example, 2000 yen) pays and an event (a. pay2000) occurs in the condition q5, it will change to a condition q7. In the condition q7, if a copy event (copy) occurs, it will change in this condition q7 again.

Moreover, in the condition q7, if a copy event (copy) occurs, it will change to a condition q8. In the condition q8, if a play event (play) occurs, it will change in this condition q8 again. Moreover, in this condition q8, if a copy event (copy) occurs, it will change in the condition q9. It is in the termination condition that it changes to no condition and an event cannot be generated in the condition q9, either. That is, with this automaton, if payment of 2000 yen is carried out, it is shown that a music content can be copied to other devices without a count limit. Moreover, with this automaton, although any number of times of reproducing the copied music content are possible, when it copies to other devices etc., it is shown that playback becomes impossible.

[0214] And when a tuple train describes the automaton which carries out a state transition as mentioned above, it comes to be shown in drawing 13 .

[0215] Moreover, the automaton description section 341 may describe juxtaposition composition of operating state in order to update actuation of a music content. For example, juxtaposition composition with actuation a0 and actuation a1 is expressed with a tuple train as follows.

Action accompanying a state transition may be described in <q0, alpha, and a0.q0> <q0, alpha, a1.q0> and the automaton description section 341. For example, action is expressed with tuple as follows.

<q0, alpha, q1;action> This action is expressed as a function using the variable defined beforehand. Moreover, a variable consists of ID, a scope, and initial value. There are classes, such as the music content, an album, and the whole system, in a scope. For example, the variable showing the price of acquisition of an album (a) is set to n, and is described like a.n:=1000. Thus, an example of the automaton description section 341 action to a variable was described to be is shown below.

<q0, pay100, q1, a.n:=a.n-100> ... (1)

<q0, pay (a. n), q1, a.n:=0> ... (2)

<q1, play, q2> ... (3)

This example shows that the acquisition price {a formula (1)} of one music content affects the price of album acquisition {a formula (2)}.

[0216] The above automaton description sections 341 consist of an entry ID 345, content ID 346, version information 347, variable information 348, and a tuple train 349, as shown in drawing 14 .

[0217] The example of the automaton description section 341 in which the description format was defined as mentioned above is explained.

[0218] In addition, the event and command which are used for below by description of an automaton are defined by DTD (Document Type Definition) specified based on the specification of XML. For example, as shown in drawing 15 , a playback actuation (play), duplicate actuation (copy), right purchase (pay-for-play) of playback, right-of-reproduction-copyright purchase (pay-for-copy), right purchase (pay-for-album-play) of album playback, album right-of-reproduction-copyright purchase (pay-for-album-copy), usable opening day (from), and use end date (to) and the Nur actuation (null) are defined by DTD as an event.

[0219] Drawing 16 is the example of description of the automaton description section 341 by the XML language which shows that a music content can be reproduced from September 1, 1999.

[0220] The description shown in this drawing 16 serves as an automaton as shown in drawing 17 . This automaton consists of a condition q1 of an initial state, and a condition q2. In the condition q1, if the date is set to September 1, 1999 of an usable opening day (from), it will change to a condition q2. And in the condition q2, if a playback event (play) occurs, a music content will be reproduced and it will change to a condition q2 again. Thus, this automaton is controlled to enable September 1, 1999 to playback for a music content.
[0221] Drawing 18 is the example of description of the automaton description section 341 by the XML language which shows that a music content can be reproduced till October 31, 1999.
[0222] The description shown in this drawing 18 serves as an automaton as shown in drawing 19 . This automaton consists of a condition q1 of an initial state, and a condition end of a termination condition. In the condition 2, if a playback event (play) occurs, a music content will be reproduced and it will change to a condition q2 again. Moreover, in the condition 2, if October 31, 1999 of a use end date (to) comes, it will change to Condition end. When it comes to Condition end, it changes to no condition and an event is not generated, either. Thus, this automaton is controlled to make playback possible for a music content till October 31, 1999.
[0223] Drawing 20 is the example of description of the automaton description section 341 by the XML language which shows that the refreshable period of a music content is from September 1, 1999 to October 31, 1999, and the count of refreshable is 16 times.
[0224] The description shown in this drawing 20 serves as an automaton as shown in drawing 21 . This automaton consists of a condition q1 of an initial state, a condition q2, and a condition end of a termination condition. In the condition q1, if September 1, 1999 of an usable opening day (from) comes, it will change to a condition q2. And in the condition q2, if a playback event (play) occurs, a music content will be reproduced and it will change to a condition q2 again. Moreover, if October 31, 1999 of a use end date (to) comes or a playback event (playx16) occurs 16 times in the condition 2, it will change to Condition end. When it comes to Condition end, it changes to no condition and an event is not generated, either. Thus, this automaton carries out the playback period of a music content to from September 1, 1999 to October 31, 1999, and is controlling that count of playback to 16 times.
[0225] Drawing 22 is the example of description of the automaton description section 341 by the XML language which shows that the count of playback of a music content is restricted to 16 times.
[0226] Next, as shown in drawing 23 , the certificate of attestation 354 for verifying the signature 353 of the parameter description section 351, the authorization code 352 with a contents key, and a contents provider and this signature is added to the parameter file 333. Here, a contents provider's private key and public key which created KC and contents for the contents key are set to K-1E and K1E, respectively.
[0227] Moreover, a parameter file 333 can be rewritten by the contents provider (for example, secondary providers, such as a contents retailer and a contents middle contractor) other than the contents provider who created the above-mentioned automaton file 332. As the rewritten parameter file 333 is shown in drawing 24 , the unique entity ID 55 given to each provider, middle contractor, etc. is added. Here, K'C is a secondary provider's contents key and serves as K'C=H (KC, EntityID). In addition, H

is an one-way hash function here. A secondary provider's contents key K'C is created from a primary provider's contents key KC. A primary provider and a secondary provider are distinguished with the certificate of attestation.
[0228] If the contents key is obtained, when MAC will perform and a contents key will not be obtained by the reasons of safety etc. as an approach of verifying a parameter file 333, it verifies with a signature and a certificate.
[0229] The protocol verified by MAC is as follows. S and a secondary provider are set to A and a terminal is set to B for the primary provider of contents. S->A shows transmission to A from S, S->B shows transmission to B from S, and A->B shows transmission to B from A. Moreover, IDA shows ID of Device A.
[0230] S->A: K'C=H (KC, IDA)
S->B: X=EKs (KC)
A->B: IDA, Parameters, M=MACK'C (Parameters)
B: M MACK'c (Parameters).
The multiplier of the function for modification of the value described by the automaton section 41 of the above-mentioned automaton file 31 is described by this parameter description section 351. For example, in the example shown in drawing 13 , the price of a music content may serve as a function as follows in the automaton section 41, for example.
< -- q0, pay (f1 (10)), and q1> <q1, pay (f2 (10) xn), q2> -- this case -- the above-mentioned functions f1 and f2 -- for example, it sets as follows.
f1(n) =0.9nf2 (n) = -- by defining 90+0.1n of functions in this way, for example, a primary provider defines the default of a price, and a secondary provider can rewrite a parameter file 333 and can change a price.
[0231] The above parameter description sections 351 consist of an entry ID 356, content ID 357, and multiplier information 358, as shown in drawing 25 .
[0232] A history file 334 is a file which describes the locus of actuation of the music content which operates based on the contents of description in the automaton description section 341. The status and the variable in tuple of the above-mentioned automaton description 41 are recorded on this history file 334. For example, when playback is performed twice to drawing 13 mentioned above in an example, it is set to <q0, q1, q0, q1>, and, thereby, the locus of the following actuation can be obtained. <pay10, play, pay10, play> If this is totaled, for example, upload etc. is carried out to the comprehension management unit (X) 315, a user can pay and the amount of money can be calculated.
[0233] As mentioned above, in a music content distribution system, since the automaton which programmed the policy itself and its concrete value has described use condition information, the degree of freedom of a publication of the use conditions of contents can be raised.
[0234] (4) restoration of the destroyed music content, and re-download -- next, explain backup of the music content by the comprehension management unit (X) 315.
[0235] First, the key management method of the music content of the comprehension management unit (X) 315 is explained using drawing 26 .
[0236] The comprehension management units (X) 315 are music contents C1, C2, and C3 to HDD21 in a personal computer 1... Cn is stored. Moreover, the comprehension management units (X) 315 are each music contents C1, C2, and C3... They are the

contents keys Kc1, Kc2, and Kc3 corresponding to Cn... Kcn is also stored. The contents key Kc serves as relation of one to one to music content C. Moreover, each music contents C1, C2, and C3 ... The content ID for [each] identifying is added to Cn. It is this content ID CID1, CID2, and CID3 ... It is referred to as CIDn.
[0237] Music contents C1, C2, and C3 ... Cn is the contents keys Kc1, Kc2, and Kc3... It is enciphered by Kcn and they are E (Kc1, C1), E (Kc2, C2), and E (Kc3, C3)... It is recorded in HDD21 of a personal computer 1 in the condition of having been referred to as E (Kcn, Cn). Here, E (K, C) shows that Contents C are enciphered with Key K. Usually, content ID is made into the condition that it is recorded on the header of music content C etc., and is enciphered with music content C, or MAC was added to music content C, and separation has become impossible with the music content body.
[0238] Moreover, contents keys Kc1, Kc2, and Kc3 ... It is enciphered with the storage key KS and Kcn is E (KS, Kc1), E (KS, Kc2), and E (KS, Kc3)... It is recorded on HDD21 of a personal computer 1 in the condition of having been referred to as E (KS, Kcn). This storage key KS has the so-called Tampa-proof nature, and is saved from the regular user in the record section which cannot be referred to.
[0239] In the comprehension management unit (X) 315 to which key management is performed as mentioned above, in reproducing a music content C1, the code of the contents key Kc1 is canceled using the storage key KS, then it cancels the code of a music content C1 using this contents key Kc1, for example. By this, the comprehension management unit (X) 315 can reproduce a music content C1.
[0240] moreover, in the comprehension management unit (X) 315 to which key management is performed as mentioned above for example, portable [from HDD21] in a music content C1, in moving to (Device X) 6-3 (MOVE) Portable device (X) If mutual recognition is performed among 6-3 and authentication is completed, the code of the contents key Kc1 will be canceled using the storage key KS. then, the contents key Kc1 is enciphered with a session key, and portable in the enciphered contents key Kc1 and the enciphered music content C1 -- it transmits to (Device X) 6-3. And elimination is carried out for both the music contents C1 to the contents key Kc1 from HDD21. by this, the comprehension management unit (X) 315 is portable in a music content C1 -- it can move to (Device X) 6-3.
[0241] Below, when HDD21 breaks, the restoration approach of a music content when it becomes impossible to reproduce a music content and a contents key from HDD21 is explained.
[0242] First, the comprehension management unit (X) 315 usually sometimes saves the backup data of enciphered music content C and the contents key Kc at the inside of HDD21, other record media, etc.
[0243] Moreover, the comprehension management unit (X) 315 usually sometimes manages the record of purchase of a music content downloaded from -3, and the list of the content ID of all the music contents memorized in EMD (server X) 4HDD21 as use log information. this log information is portable when a music content is downloaded from EMD (server X) 4-3 -- it is made to update when music contents, such as migration to (Device X) 6-3, are controlled Moreover, log information is stored in another field and other record media of HDD21. The comprehension management unit (X) 315 uploads this log information to EMD (server X) 4-3, periodical or whenever it accessed.

[0244] And when music content C and the contents key Kc which are stored in HDD21 of the comprehension management unit (X) 315 have been destroyed, processing as shown below is performed.
[0245] When music content C and the contents key Kc have been destroyed, first, the comprehension management unit (X) 315 accesses EMD (server X) 4-3, and performs user authentication.
[0246] Then, EMD (server X) 4-3 generate the adjustment verification value ICV (Integrity Check Value) from a user's attested user ID with reference to the use log information of the comprehension management unit (X) 315. This adjustment verification value ICV is generated as follows based on CID which is the content ID of music content C described by use log information, and the storage key KS of the comprehension management unit (X) 315. ICV=H (KS, CID1||CID2|| ... ||CIDn) -- here, H (K, Data) is an one-way hash function, and the value changes with keys K.
[0247] Then, EMD (server X) 4-3 transmit the generated adjustment verification value ICV to the comprehension management unit (X) 315.
[0248] Then, if music content C or the contents key Kc is backed up, the comprehension management unit (X) 315 restores the backup data, and saves music content C or the contents key Kc in HDD21. Moreover, if music content C or the contents key Kc is not backed up, I have music content C or the contents key Kc destroyed from EMD (server X) 4-3 re-distributed. Accounting will not be performed if EMD (server X) 4-3 are contents purchased with reference to a user's purchase hysteresis before at this time.
[0249] The comprehension management unit (X) 315 performs the above processing, and revives destroyed music content C or the contents key Kc.
[0250] And the comprehension management unit (X) 315 checks CID of the music content with the above-mentioned adjustment verification value ICV, when performing playback and control of revitalized music content C or the contents key Kc. Thus, by checking music content C or the contents key Kc revived using the adjustment verification value ICV for example, portable in a certain music content Ci -- from HDD21, by moving to (Device X) 6-3, when eliminated Even if it keeps in mind E (Kci, Ci) which is the music content Ci as which the malicious user was enciphered and restores, that those data are reproduced cannot control migration etc., either.
[0251] In addition, when music content C and not the contents key Kc but the storage key KS is destroyed, re-install of the comprehension management unit (X) 315 is performed. If log information is uploaded while carrying out user registration to EMD (server X) 4-3 even if it is this case, restoration and re-download can be carried out by the approach mentioned above.
[0252] Thus, it can restore in a music content distribution system, protecting copyright by crash of a hard disk etc., for example, even if it is the case where the music content has been destroyed. For example, if the music content purchases to normal, it can be made to revive for nothing.
[0253] (5) comprehension -- management -- a unit -- a master -- a key -- and -- authentication -- a key -- etc. -- distribution -- an approach -- comprehension -- management -- a unit -- (-- X --) -- 315 -- portable -- a device -- (-- X --) -- six - three -- between -- **** -- portable -- a device -- (-- X --) -- six - three -- a proper -- ID -- and -- authentication -- a key (MG-ID/IK) -- comprehension -- management -- a unit -- (-- X --) -

- 315 -- a proper -- a master -- a key (OMG-MK) -- using -- mutual recognition -- carrying out -- having .
[0254] as portable as the comprehension management unit (X) 315 -- portable [from the comprehension management unit (X) 315] among (Device X) 6-3, when mutual recognition is performed -- portable in transmitting a music content to (Device X) 6-3 (check-out) -- the music content from (Device X) 6-3 to the comprehension management unit (X) 315 can be returned now (check-in). in addition, the comprehension management unit (X) 315 saves the music content enciphered in HDD21 of a personal computer 1, and is portable -- (Device X) 6-3 save the music content enciphered to storages, such as an internal memory card. therefore, portable from the comprehension management unit (X) 315 -- when transmitting a music content to (Device X) 6-3, the music content on HDD21 of a personal computer 1 is portable -- it will be transmitted on the memory card with which (Device X) 6-3 were equipped. moreover, portable -- portable, when transmitting a music content to the comprehension management unit (X) 315 from (Device X) 6-3 -- the music content on the memory card with which (Device X) 6-3 were equipped will be transmitted on HDD21 of a personal computer 1.
[0255] Portable device (X) 6-3 has held beforehand ID information (MG-ID), the authentication key (MG-IK) for two or more generations, and the master key (OMG-MK) for two or more generations from the time of factory shipments. Portable device (X) These keys etc. are not behind supplied to 6-3 from the exterior. Portable device (X) 6-3 updates the generation of an authentication key (MG-IK) and a master key (OMG-MK) if needed. Portable device (X) 6-3 performs mutual recognition with the newest generation's authentication key and master key by which renewal of a generation was carried out, and does not perform mutual recognition with an old generation's authentication key and master key. hereafter, portable -- (Device X) 6-3 shall hold the authentication key (MG-IK [0-99]) and master key (OMG-MK [0-99]) for 100 generations of the 0th generation to the 99th generation In addition, the authentication key of the i-th generation is indicated to be (MG-IK [i]), and the master key of the i-th generation is indicated to be (OMG-MK [i]).
[0256] Moreover, the comprehension management unit (X) 315 can transmit and save a music content in a personal computer 1 from the compact disk for audios etc. by holding a master key (OMG-MK). Moreover, by holding a master key (OMG-MK), the comprehension management unit (X) 315 can download a music content from EMD (server X) 4-3, and can save it in a personal computer 1.
[0257] Here, in the comprehension management unit (X) 315, although a music content can be transmitted from a compact disk, it is that from which the master key (OMG-MK) which can transmit a music content also from EMD (server X) 4-3 differed also from the master key (OMG-MK) which cannot download a music content, and the compact disk from EMD (server X) 4-3. Hereafter, although a music content can be transmitted from a compact disk, from EMD (server X) 4-3, the thing of the key which cannot download a music content is also called key only for ripping, and the thing of a key which can transmit a music content also from EMD (server X) 4-3 is also called EMD key also from a compact disk.

[0258] In addition, in this example, the master key (OMG-MK [0]) of the 0th generation is a key only for ripping, and the master key after the 1st generation (OMG-MK [1-99]) is an EMD key.
[0259] Below, the procedure of processing in which the key only for ripping was used is explained.
[0260] portable in CD-ROM361 in which the install software of the comprehension management unit (X) 315 was stored, as shown in drawing 27 , when the comprehension management unit (X) 315 is installed from CD-ROM -- (Device X) 6-3 and the floppy (trademark) disk 362 are sold by the set. portable in a floppy disk 362 -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [0]) of the 0th generation, and the master key (OMG-MK [0]) of the 0th generation are stored.
[0261] Then, in order to make usable the sold portable (device X) 6-3 grade, a personal computer 1 is first equipped with CD-ROM361 (step S11). Then, the comprehension management unit (X) 315 is installed in a personal computer 1 from this CD-ROM361 (step S12). Then, the comprehension management unit (X) 315 will be stored in the hard disk of a personal computer 1 (step S13). then, it is stored in the floppy disk 362 -- portable -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [0]) of the 0th generation, and the master key (OMG-MK[0]) of the 0th generation are saved in a personal computer 1 (step S14).
[0262] By this, the comprehension management unit (X) 315 can store now the music content offered by music CD363 grade in the hard disk of a personal computer 1 (step S15). In addition, since the master key (OMG-MK [0]) of the 0th generation is a key only for ripping, it can download a music content no longer from EMD (server X) 4-3.
[0263] moreover, portable -- although (Device X) 6-3 hold the authentication key and master key for 100 generations with which renewal of a generation is carried out inside, they are made into the 0th generation in the state of initialization. for this reason, as portable as the comprehension management unit (X) 315 holding the authentication key of the 0th generation, and a master key -- the mutual recognition of (Device X) 6-3 becomes possible. therefore, portable in the music content offered by music CD363 grade -- it can store now in the memory card of (Device X) 6-3 (step S16).
[0264] portable, as it is shown in drawing 28 on the other hand, when the comprehension management unit (X) 315 is offered through a network -- the address, user ID, a password, etc. of the EMD registration server 3 on the Internet are offered with (Device X) 6-3.
[0265] Then, in order to make usable the sold portable (device X) 6-3 grade, the EMD registration server 3 on a network is first accessed using user ID and a password (step S21). Then, the EMD registration server 3 performs authentication of user ID and a password (step S22). then, if there is no problem in authentication, the EMD registration server 3 is as portable as the install software of the comprehension management unit (X) 315 -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [0]) of the 0th generation, and the master key (OMG-MK [0]) of the 0th generation are transmitted to a personal computer 1 (step S23). then, a personal computer 1 is portable while it starts the install software of the comprehension management unit (X) 315 and installs the comprehension management unit (X) 315 -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [0]) of the 0th generation, and the

master key (OMG-MK [0]) of the 0th generation are saved at HDD21 (step S24). Then, the comprehension management unit (X) 315 will be stored in a hard disk (step S25).
[0266] By this, the comprehension management unit (X) 315 can store now the music content offered by music CD363 grade in HDD21 of a personal computer 1 (step S26). In addition, since the master key (OMG-MK [0]) of the 0th generation is a key only for ripping, it can download a music content no longer from EMD (server X) 4-3.
[0267] moreover, portable -- although (Device X) 6-3 hold the authentication key and master key for 100 generations with which renewal of a generation is carried out inside, they are made into the 0th generation in the state of initialization. for this reason, as portable as the comprehension management unit (X) 315 holding the authentication key of the 0th generation, and a master key -- the mutual recognition of (Device X) 6-3 becomes possible. therefore, portable in the music content offered by music CD363 grade -- it can store now in the memory card of (Device X) 6-3 (step S27).
[0268] In addition, it is not restricted to the approach shown in the above drawing 27 and drawing 28 , but the comprehension management unit (X) 315 and the master key of the 0th generation only for ripping (OMG-MK [0]) are stored in CD-ROM361, and portable ID for authentication with (Device X) 6-3 and the authentication key (MG-ID/IK) of the 0th generation may be offered through a network.
[0269] Below, the key only for ripping is updated in an EMD lock at a key, and the procedure of processing of enabling it to deal with the music content downloaded from EMD (server X) 4-3 is explained.
[0270] By the procedure shown in drawing 27 or drawing 28 , the comprehension management unit (X) 315 is offered through networks, such as removable media, such as CD-ROM, and the Internet, and is installed in HDD21 in a personal computer 1. at this time, the comprehension management unit (X) 315 holds the master key (OMG-MK [0]) of the 0th generation which is exclusively for ripping, and ID for authentication and the authentication key (MG-ID/IK [0]) of the 0th generation, and is portable -- he is also the generation of the key of (Device X) 6-3 in the default state.
[0271] First, a personal computer 1 accesses the EMD registration server 3 on a network using user ID and a password, as shown in drawing 29 (step S31). Then, the EMD registration server 3 performs authentication of user ID and a password (step S32). Then, if there is no problem in authentication, the EMD registration server 3 will register ID information (OMG-ID) on a personal computer 1, and will generate the certificate of attestation (Cert [PK]) of a public key (OMG-PK) for the comprehension management unit (X) 315 to connect with EMD (server X) 4-3, a private key (OMG-KS), and a public key (step S33). Then, the EMD registration server 3 transmits the certificate of attestation (Cert [PK]) of the generated public key (OMG-PK), a private key (OMG-KS), and a public key to a personal computer 1 (step S34).
[0272] then, the EMD registration server 3 is portable -- ID information (MG-ID) on (Device X) 6-3, the authentication key (MG-IK [i]) of the i-th generation, and the master key (OMG-MK [i]) of the i-th generation are transmitted to a personal computer 1 (step S35). Then, the comprehension management unit (X) 315 of a personal computer 1 carries out renewal of a generation of these keys at the i-th generation based on received ID information (MG-ID), the authentication key (MG-IK [i]) of the i-th generation, and the master key (OMG-MK [i]) of the i-th generation (step S36). then, the comprehension management unit (X) 315 is portable -- it attests among (Device X) 6-3

(step S37). Portable device (X) 6-3 will update the generation of a self key to the i-th generation, if authentication is carried out (step S38).
[0273] By this, the comprehension management unit (X) 315 can store in HDD21 of a personal computer 1 the music content which carried out the Dow-Jones load from EMD (server X) 4-3 while being able to store the music content offered by music CD363 grade in the hard disk of a personal computer 1.
[0274] Below, the procedure which carries out renewal of a generation of an EMD key etc. is explained.
[0275] the comprehension management unit (X) 315 holds the master key (OMG-MK[i]) of the i-th generation, and ID for authentication and the authentication key (MG-ID/IK [i]) of the 0th generation, and is portable -- the generation of the key of (Device X) 6-3 is also the i-th generation.
[0276] First, if the EMD registration server 3 is accessed since a personal computer 1 is a certain processing as shown in drawing 30 , the EMD registration server 3 will attest ID of the comprehension management unit (X) 315, and will transmit a ** (i+k) generation's authentication key (MG-IK [i+k]), and a ** (i+k) generation's master key (OMG-MK [i+k]) to a personal computer 1 (step S41). Then, the comprehension management unit (X) 315 of a personal computer 1 updates the authentication key and master key which were received in a ** (i+k) generation (step S42). then, the comprehension management unit (X) 315 is portable -- (Device X) 6-3 and authentication are performed (step S43). Portable device (X) 6-3 will update the generation of a self key in a ** (i+k) generation from the i-th generation, if authentication is carried out (step S44).
[0277] moreover, portable on the other hand, as shown in drawing 31 -- portable, when the generation of the authentication key which (Device X) 6-3 use is a ** (i+k) generation and the generation of the authentication key which the comprehension management unit (X) 315 holds is the i-th generation -- it will become authentication failure if authentication with (Device X) 6-3 and the comprehension management unit (X) 315 is performed (step S51). If authentication goes wrong, the comprehension management unit (X) 315 will perform a key demand to the EMD registration server 3 (step S52). If there is a key demand, the EMD registration server 3 will attest ID of the comprehension management unit (X) 315, and will transmit a ** (i+k) generation's authentication key (MG-IK [i+k]), and a ** (i+k) generation's master key (OMG-MK [i+k]) (step S53). Then, the comprehension management unit (X) 315 updates the authentication key and master key which were received in a ** (i+k) generation (step S54). then, the comprehension management unit (X) 315 is portable -- (Device X) 6-3 and authentication are performed (step S55).
[0278] By this, the comprehension management unit (X) 315 can store in HDD21 of a personal computer 1 the music content downloaded from EMD (server X) 4-3 while being able to store the music content offered by music CD363 grade in the hard disk of a personal computer 1 (step S38).
[0279] as mentioned above -- a music content distribution system -- the comprehension management unit (X) 315 -- and portable -- he divides into the key and server connection key only for ripping the master key and authentication key which (Device X) 6-3 use, and is trying to download a server connection key through a network further For this reason, in a music content distribution system, even if the safety of the music

content distributed from the server increases, for example, the key only for ripping is torn, the music content downloaded from a server cannot be broken.
[0280] moreover -- a music content distribution system -- the comprehension management unit (X) 315 -- and portable -- renewal of a generation is carried out and the master key and authentication key which (Device X) 6-3 use are used. Furthermore, a master key and an authentication key are supplied through a network, and the comprehension management unit (X) 315 performs renewal of a generation. For this reason, the safety of a music content increases.
[0281]
[Effect of the Invention] According to this invention, a data processor performs playback and/or control of restoration of backup, or the re-distributed contents data based on the use log information re-acquired from the contents server.
[0282] By this, the contents data which carried out contents distribution through the network can restore contents data by this invention, aiming at protection of copyright, even if it is the case where it has once been destroyed.
DESCRIPTION OF DRAWINGS
[Brief Description of the Drawings]
[Drawing 1] It is drawing showing the music content distribution structure of a system of the gestalt of operation of this invention.
[Drawing 2] It is drawing showing the configuration of the personal computer in the above-mentioned music content distribution system.
[Drawing 3] It is drawing showing the configuration of the portable device in the above-mentioned music content distribution system.
[Drawing 4] It is drawing explaining the function of the above-mentioned personal computer.
[Drawing 5] It is drawing showing an example of a display operator guidance window.
[Drawing 6] A sound recording program is drawing showing the example of a display displayed on a display.
[Drawing 7] It is drawing for explaining the unific handling of the contents from which a format differs for every distribution contractor in the above-mentioned music content distribution system.
[Drawing 8] It is drawing explaining the relation between a unification transfer protocol layer and an application layer.
[Drawing 9] It is drawing explaining a format of the use condition information that it is generally used.
[Drawing 10] It is drawing explaining the file which constitutes the unification use condition information that it is used in a comprehension management unit.
[Drawing 11] It is drawing explaining the configuration of the automaton file of the above-mentioned unification use condition information.
[Drawing 12] It is drawing explaining an example of the automaton in which transition of the music content described by the automaton description section of the above-mentioned automaton file of operation is shown.
[Drawing 13] It is drawing which expressed the above-mentioned automaton in the tuple train.
[Drawing 14] It is drawing explaining the configuration of the above-mentioned automaton description section.

[Drawing 15] It is drawing showing the event defined by DTD specified based on the specification of XML, and a command.
[Drawing 16] It is drawing showing the 1st example of description of the above-mentioned automaton description section.
[Drawing 17] It is the state transition diagram of the example of description of the above 1st.
[Drawing 18] It is drawing showing the 2nd example of description of the above-mentioned automaton description section.
[Drawing 19] It is the state transition diagram of the example of description of the above 2nd.
[Drawing 20] It is drawing showing the 3rd example of description of the above-mentioned automaton description section.
[Drawing 21] It is the state transition diagram of the example of description of the above 3rd.
[Drawing 22] It is drawing showing the 4th example of description of the above-mentioned automaton description section.
[Drawing 23] It is drawing explaining the configuration of the parameter file of the above-mentioned unification use condition information.
[Drawing 24] It is drawing explaining the configuration at the time of updating the above-mentioned parameter file.
[Drawing 25] It is drawing explaining the configuration of the parameter description section of the above-mentioned parameter file.
[Drawing 26] It is drawing explaining the management method of the contents by the above-mentioned comprehension management unit.
[Drawing 27] It is drawing explaining procedure in case a comprehension management unit is installed from CD-ROM.
[Drawing 28] It is drawing explaining procedure in case a comprehension management unit downloads and is installed from a network.
[Drawing 29] It is drawing explaining the update procedure updated in an EMD lock from a ripping key.
[Drawing 30] It is drawing explaining the 1st example of the procedure which updates an EMD key.
[Drawing 31] It is drawing explaining the 2nd example of the procedure which updates an EMD key.
[Description of Notations]
1 Personal Computer, 2 Network, 3 EMD Registration Server, 4EMD Server, 6 Portable Device, 7 USB Interface, 21 Hard Disks, 311,312 Application for Playback, 313,314 Device Drivers, 315 Comprehension Management Unit, 316 Reception Interface for EMD, 317 Transmitting Interface for EMD, 318 PD Driver